NPS ARCHIVE
1998.09
THIRY, D.

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

MIGRATING FROM WIN NT 4.0 TO WIN NT 5.0 IN THE MARINE CORPS ENTERPRISE NETWORK (MCEN)

by

Douglas B. Thiry
and
Robert A. Rowlette

September 1998

Thesis Advisor: Doug Brinkley

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1998	Master's Thesis

4. TITLE AND SUBTITLE : MIGRATING FROM WIN NT 4.0 TO WIN NT 5.0 IN THE MARINE CORPS ENTERPRISE NETWORK (MCEN)

5. FUNDING NUMBERS

6. AUTHOR(S)
Thiry, Douglas B. and Rowlette, Robert A.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The purpose of this study is to provide the United States Marine Corps (USMC) with an analysis of Windows NT 5.0 Network Operating System (NOS). This analysis will assist the Network Operations Center (NOC) in preparation for the eventual migration of Windows NT 5.0 into the Marine Corps Enterprise Network (MCEN).

NT 5.0 offers some significant enhancements over earlier versions. Active Directory provides a unified platform to manage NOS resources by storing user information, network shares and policies. NT File System (NTFS) version 5 permits dynamic allocation of primary storage space to each user. NT 5.0 also improves network security by incorporating use of the Kerberos Version 5 protocol, providing integrated security for authentication and file encryption.

A top-down migration strategy should be incorporated by the NOC. Particularly important is how the NOC builds the Domain Naming Service (DNS) conventions for the MCEN. This will require every subordinate unit to adhere to the naming convention of its chain of command.

Migrating from Banyan Vines to Windows NT presents a significant change to the organization. An effective Change Management strategy can assist members of the organization in understanding the sense of loss and uncertainty that occur in times of transition, and to deal with these changes effectively.

14. SUBJECT TERMS
USMC, Marine Corps Enterprise Network, MCEN, Network Operations Center, NOC, Network Operating System, NOS, WIN NT 5.0, NT, Change Management

15. NUMBER OF PAGES
115

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	21. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

MIGRATING FROM WIN NT 4.0 TO WIN NT 5.0 IN THE MARINE CORPS ENTERPRISE NETWORK (MCEN)

Douglas B. Thiry
Captain, United States Marine Corps
B.S., United States Naval Academy, 1989

Robert A. Rowlette
Major, United States Marine Corps
B.A., University of Florida, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1998

ABSTRACT

The purpose of this study is to provide the United States Marine Corps (USMC) with an analysis of Windows NT 5.0 Network Operating System (NOS). This analysis will assist the Network Operations Center (NOC) in preparation for the eventual migration of Windows NT 5.0 into the Marine Corps Enterprise Network (MCEN).

NT 5.0 offers some significant enhancements over earlier versions. Active Directory provides a unified platform to manage NOS resources by storing user information, network shares and policies. NT File System (NTFS) version 5 permits dynamic allocation of primary storage space to each user. NT 5.0 also improves network security by incorporating use of the Kerberos Version 5 protocol, providing integrated security for authentication and file encryption.

A top-down migration strategy should be incorporated by the NOC. Particularly important is how the NOC builds the Domain Naming Service (DNS) conventions for the MCEN. This will require every subordinate unit to adhere to the naming convention of its chain of command.

Migrating from Banyan Vines to Windows NT presents a significant change to the organization. An effective Change Management strategy can assist members of the organization in understanding the sense of loss and uncertainty that occur in times of transition, and to deal with these changes effectively.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1
B. OBJECTIVES 3
C. RESEARCH QUESTION 3
D. SCOPE, LIMITATIONS, ASSUMPTIONS 4
1. Scope 4
2. Limitations 5
3. Assumptions 6
E. ORGANIZATION OF STUDY AND CONTRIBUTIONS 6
1. USMC & MCEN Overview (Chapter II) 6
2. Technical Developments (Chapter III) 7
3. Migration (Chapter IV) 7
4. Change Management (Chapter V) 7
5. Conclusions And Recommendations (Chapter VI) 8

II. USMC & MCEN OVERVIEW 9

A. ORGANIZATION OF THE MARINE CORPS 9
1. Headquarters, United States Marine Corps 10
2. Headquarters, Marine Forces 10
3. Marine Expeditionary Forces 11
4. Marine Forces, Reserve 13
5. Marine Corps Systems Command 14
B. MARINE CORPS ENTERPRISE NETWORK (MCEN) 14
C. CURRENT ENVIRONMENT 15
1. Network Operating System 15
2. Routers 15
3. Messaging 16
4. Directory Services 17
5. User Desktop 17
6. Remote Access 18
7. 3270-Based Mainframe Access 18
8. Legacy Services 19
9. Lotus Notes 19
D. MIGRATING THE MCEN 20
E. SUMMARY 21

III. TECHNICAL DEVELOPMENTS 23

A. ACTIVE DIRECTORY 24
1. NT 4.0 Databases 25
2. Directory Services 27

3. Active Directory Features 30
4. Microsoft Management Console 36
B. NTFS 5 37
1. Volume Management 38
2. Quota Support 39
3. Hierarchical Storage Management (HSM) 39
4. Security 40
C. SECURITY 41
1. Kerberos Authentication 41
2. Encrypted Files System (EFS) 44
D. HARDWARE 45
1. Server Components 45
2. Network Resources 45
E. SUMMARY 46

IV. MIGRATION 49

A. OVERVIEW 49
1. Assumptions 49
2. Configuration 51
B. PLANNING 51
1. Domain model 52
2. TCP/IP 54
3. DHCP/WINS 54
4. NT DNS Server 55
5. Determine NT 5.0 Configuration 56
6. DCs 58
7. Third Party Influences 59
8. PC Lab 60
9. MCEN Example 60
C. EXECUTE THE UPGRADE 62
1. NT 4.0 (Upgrade) 63
2. PDC 64
3. BDC 67
4. Stand-Alone or Member Servers 68
5. New Installation 68
6. Post Upgrade Actions 69
7. Observations 69
D. MCEN IMPLICATIONS 71
1. Domain Tree Configuration 71
2. DNS 74
3. Active Directory 78
4. NTFS 79
E. SUMMARY 80

V. CHANGE MANAGEMENT 81

A. DESCRIPTION OF USMC MIGRATION 81
1. USMC Organization 81
2. Migration Strategy Development 82
B. TRANSITION MANAGEMENT 83
1. Permanent White Water 84
2. Endings, Neutral Zone and New beginnings 84
3. Communicating The Transition 86
C. USMC TRANSITION 87
1. Communicate Early and Often 89
2. Communicate Your Destination 89
3. Create Messages That Motivate 89
4. Build Commitment Interactively 90
D. SUMMARY 90

VI. CONCLUSIONS AND RECOMMENDATIONS 91

A. CONCLUSIONS 91
1. NT 5.0 Improvements over NT 4.0 91
2. Centralized Coordination, Decentralized Execution 91
3. DII COE Compliance And Joint Interoperability 91
B. RECOMMENDATIONS 92
C. AREAS FOR FURTHER RESEARCH 92
1. Evaluating NT 5.0 92
2. Certificate Servers in the MCEN 93
3. Security Concerns with NT 93
4. X.500 Capability for the MCEN 93

LIST OF REFERENCES 95

INITIAL DISTRIBUTION LIST 97

LIST OF FIGURES

Figure 1. Major Marine Corps commands 9
Figure 2. Typical Marine Expeditionary Force 13
Figure 3. Typical Marine division organizational chart 13
Figure 4. WAN router sites 16
Figure 5. NOS Market Base 23
Figure 6. The Active Directory service interacts with all other network services. 25
Figure 7. DNS is the Windows NT Locator Service 31
Figure 8. Child domains inherit their parent's DNS name. 35
Figure 9. Active Directory uses a hierarchy of domain trees, domains, and OUs. 35
Figure 11. The MMC tool. 37
Figure 13. Numerous trust relationships are required in NT 4.0 42
Figure 15. Domain in a tree share transitive trust relationships. 43
Figure 17. Organizational hierarchy 50
Figure 18. Single Domain 53
Figure 19. Master domain with resource domain 53
Figure 20. Joining a the MCEN domain tree 62
Figure 21. MCEN DNS namespaces 77

LIST OF TABLES

Table 1. Minimum server hardware list. 45
Table 2. Hardware configuration for test PC 51
Table 3. List of Losses 88

LIST OF ACRONYMS

ACL	Access Control List
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BDC	Backup Domain Controller
BN	Battalion
CINC	Commander in Chief
COMMARFORLANT	Commander, Marine Forces Atlantic
COMMARFORPAC	Commander, Marine Forces Pacific
COTS	Commercial Off-the-Shelf
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DII-COE	Defense Information Infrastructure-Common Operating Environment
DISA	Defense Information Systems Agency
DIV	Division
DNS	Domain Name Service
DoD	Department of Defense
DON	Department of the Navy
EFS	Encrypting File System
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
GUI	Graphical User Interface
HQMC	Headquarters Marine Corps
HSM	Hierarchical Storage Management
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IT	Information Technology
KDC	Key Distribution List
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAGTF	Marine Air Ground Task Force
MARCORSYSCOM	Marine Corps Systems Command
MARFORLANT	Marine Forces Atlantic
MARFORPAC	Marine Forces Pacific
MARFORRES	Marine Forces Reserve
MARS	Multicast Address Resolution
MB	Megabyte
MCEN	Marine Corps Enterprise Network
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MMC	Microsoft Management Console

NIPRNET	Non-secure IP (Internet Protocol) Router Network
NOC	Network Operations Center
NOS	Network Operating System
NTFS	NT File System
NTLM	NT Logon Manager
OMFTS	Operational Maneuver From the Sea
OU	Organizational Units
PACOM	Pacific Command
PC	Personal Computer
PDA	Personal Digital Assistant
PDC	Primary Domain Controller
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
RAID	Redundant Array Independent Devices
RAM	Random Access Memory
RAS	Remote Access Server
SAM	Security Accounts Manager
SID	Security ID
SIPRNET	Secret IP (Internet Protocol) Router Network
SMTP	Simple Mail Transfer Protocol
STDA	Street Talk Directory Service
TCP	Transmission Control Protocol
USACOM	USA Command
USMC	United States Marine Corps
USN	Update Sequence Number
USN	United States Navy
WAN	Wide Area Network
WIN 95	Windows 95
WIN NT	Windows NT
WINS	Windows Internet Name Service

I. INTRODUCTION

A. BACKGROUND

The United States Marine Corps (USMC) is currently setting policy that will provide Information Technology (IT) direction well into the next century. The intent of this policy change is to maximize the benefits of IT, as well as to meet the operational challenges presented by Operational Maneuver From the Sea (OMTFS) and Joint Vision 2010.[1,2]

Until recently, each of the four services chose their own IT standard and developed independent policies. This approach resulted in significant interoperability problems, especially in the Joint warfighting arena. In an effort to reduce these problems the Defense Information Systems Agency (DISA) has defined joint interoperability as compliance with one of several configurations that have been formally certified as part of the Defense Information Infrastructure Common Operating Environment (DII-COE). As a Department of Defense (DoD) component, the Marine Corps is responsible for implementing IT solutions that are DII-COE compliant.

Headquarters Marine Corps (HQMC C4I) has been tasked by the Commandant to develop a migration strategy for the hardware, software and data that comprise the Marine Corps Enterprise Network (MCEN). In an effort to comply with DII-COE standards, the Network Operation Center (NOC), HQMC C4I began migrating the MCEN from a *Banyan Vines* Network Operating System (NOS) to a DII-COE compliant NOS. The USMC has adopted the Department of Navy's (DON) choice of *Windows NT*

as the DII-COE compliant NOS and started implementing Windows NT version 4.0 (NT 4.0) in FY 98. The NOC plans to migrate the MCEN from NT 4.0 to Windows NT version 5 when the next version is available on the commercial market.*

In an effort to provide the USMC with a common set of employment standards for network migration, the NOC published a technical discussion paper in May 1998.[3] Topics covered in this document include the current system environment, proposed configurations, migration component and considerations, minimum recommended configuration details, naming guidelines, and various administrative, disaster recovery and procedural guidelines. The NOC paper provides a plan for NT 4.0 base-line configurations ranging from base and operational level to network connectivity throughout the Marine Corps.

Microsoft is currently developing an upgrade to the NT operating system called Windows NT 5.0. Scheduled for release in the Spring of 2000, NT 5.0 represents significant changes to the current NOS. These changes incorporate key technical advancements, as well as important organizational and administrative changes. Incorporating NT 5.0 into the MCEN will necessitate developing another migration strategy due to the significant developments and anticipated impacts throughout the USMC.

---

* Microsoft has repeatedly delayed Beta versions of NT 5.0, which consequently delays the final retail version. The latest market estimates for the retail release of NT 5.0 is in the first half of CY 2000.

B. OBJECTIVES

The object of this study is to assist the USMC in its continuing NOS migration efforts while minimizing adverse effects caused by technical and organizational changes. Specifically, this study will identify relevant technical changes in NT 5.0, provide feasible migration solutions, and analyze the organizational effects the technical change will have on the MCEN. The authors will complete the following actions by the end of this study:

- Identify the significant technical developments in NT 5.0
- Determine which developments are relevant to the MCEN
- Recommend a migration course of action for MCEN administrators
- Identify possible areas where USMC organizations will experience problems with technical migration
- Suggest methods for minimizing the adverse affects of change on USMC organizations

C. RESEARCH QUESTION

Before the USMC upgrades the MCEN from NT 4.0 to NT 5.0 several question should be considered. This study will help to answer the following questions:

- What are the new features of NT 5.0 and how do they affect the MCEN?
- What technical actions should the USMC take to implement these new features?
- What is the best way to manage the change?

D. SCOPE, LIMITATIONS, ASSUMPTIONS

1. Scope

This thesis focuses its analysis on the actions appropriate for a battalion network administrator. While the MCEN supports all organizational levels in the USMC, the battalion organization is where the typical Marine conducts the everyday business of the Marine Corps. Most importantly, the basic *Marine* is the *User* and the battalion organization is the arena in which the Marine will use NT 5.0. With the battalion administrator and user in mind, the authors focus on the technical and administrative challenges of NT 5.0.

Some of the more important NT 5.0 developments are identified and discussed in the following chapters. Here are a few of the major developments that directly affect migration efforts:

- Improved directory services
- Internet domain naming conventions
- NT file system improvements
- Kerberos authentication

The study will not address specific security concerns for classified data. The many different rules and procedures for handling classified data across network assets exceeds the scope of this thesis.

2. Limitations

The authors were constrained by several limitations during the conduct of this study, each of which is listed below:

a) Beta Functionality

While Windows NT 5.0 Beta version 1 was used for this study, not all of the proposed functionality was working properly. This limited functionality prevented the authors from implementing several proposed capabilities. As a result, the authors were required to rely upon Microsoft documentation for a technical description and integrated the proposed capabilities into the migration strategy. Non-functional features are noted throughout the paper.

b) Available Information

The Microsoft Corporation owns the data rights to the software and tries to control adverse publicity regarding their product before its final retail release. This resulted in a lack of third party objective analysis available in the marketplace. Consequently, much of the available information about NT 5.0 features originated from Microsoft sources or Microsoft sponsored activities.

c) Funding & Facilities

Because NT 5.0 recommends at least 64 MB of RAM, the authors did not have access to enough suitable computers to simulate an enterprise environment. The authors were limited to a single domain controller with several NT 4.0/WIN 95 clients. While this worked well for many migration examples, many enterprise capabilities were

not tested in the laboratory. Capabilities such as *Global Catalogs* and *Transitive Trusts* between domains will require validation in a MCEN computer lab before implementation.

3. Assumptions

The authors assume that the reader is familiar with the basic USMC organizational structure and has worked as an NT 4.0 domain administrator in the MCEN. Additionally, this study does not address the migration from the Banyan Vines product to NT 5.0. The authors assume that the MCEN organization will upgrade from NT 4.0 to NT 5.0.

This study also assumes that the migration environment does not include classified information. While many of the migration steps recommended by the authors apply equally to unclassified and classified environments, the nature of classified information warrants a separate migration plan.

E. ORGANIZATION OF STUDY AND CONTRIBUTIONS

The following sections describe the flow of the thesis, and briefly discuss each chapter's major contribution to answering the research questions.

1. USMC & MCEN Overview (Chapter II)

In Chapter II, the migration analysis will provide a general overview of the Marine Corps and how the MCEN is integrated into the organizational structure.

2. Technical Developments (Chapter 3)

Chapter 3 will discuss the major technical developments of NT 5.0, as well as to provide an explanation as to why the USMC should upgrade to NT 5.0. These new features include:

- Active Directory. This feature provides X.500 directory services for all enterprise resources.
- NT File System. The new NTFS version 5 provides valuable benefits such as the ability to assign storage limits by user and encrypted file support.
- Internet Naming Scheme. NT 5.0 uses the Internet naming convention for all domain assets and user accounts, reducing resource ambiguity throughout the enterprise.

3. Migration (Chapter 4)

Chapter 4 describes a coordinated approach to migrating domains throughout the MCEN from NT 4.0 to NT 5.0. The authors recommend that the NOC implement top-down coordination with decentralized execution. This will enable every domain administrator to adhere to USMC guidelines while supervising their local migration effort.

4. Change Management (Chapter 5)

Chapter 5 introduces an often overlooked aspect of any IT initiative, *Change Management.* The commercial sector and the military have tried to implement countless IT programs only to have many of them fail due to poor transition management, lack of communication within the organization and/or limited user buy-in. Even the best technology plan will fail if users do not support the change initiative. This chapter briefly discusses some techniques for managers and leaders to avoid common transition pitfalls.

5. Conclusions And Recommendations (Chapter 6)

Chapter 6 provides a summary of each chapter's findings and recommendations, as well as suggestions for future research.

II. USMC & MCEN OVERVIEW

A. ORGANIZATION OF THE MARINE CORPS

This chapter provides an overview of the organization of the Marine Corps, as well as a description of the MCEN. The following sections offer a brief description of some of the major operational and support commands within the Marine Corps, as well as their location. Figure 1 depicts the location of major Marine Corps commands worldwide.

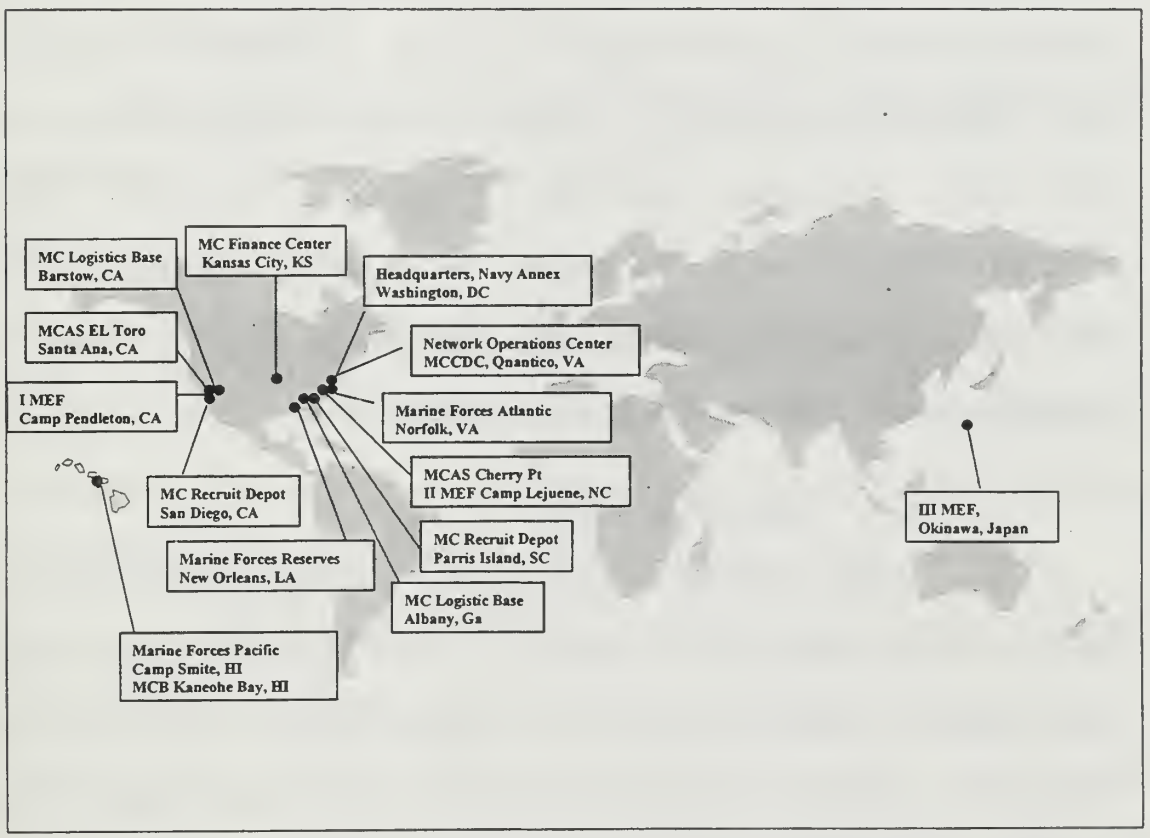

Figure 1. Major Marine Corps commands

1. Headquarters, United States Marine Corps

The Headquarters, U.S. Marine Corps (HQMC) provides leadership, doctrine, and policy for the Marine Corps. HQMC is located at the Navy Annex in Arlington, Virginia. The office of the Commandant is located nearby at the Pentagon.

2. Headquarters, Marine Forces

a) Marine Forces Atlantic

The United States Marine Corps Forces, Atlantic (MARFORLANT), headquartered at Naval Operations Base Norfolk, Virginia, is the U.S. Marine Corps component of the U.S. Atlantic Command (USACOM). MARFORLANT is one of two major Marine Corps commands that provide operating forces to support Unified or Joint Task Force Commanders and Fleet Commanders in Chief (CINCs). COMMARFORLANT serves as a principal adviser to the Commander in Chief, USACOM, on Marine Corps matters. He is responsible for organizing, training, and equipping forces for employment as directed by USACOM.[4]

b) Marine Forces, Pacific

Marine Forces Pacific (MARFORPAC), headquartered at Camp Smith, Hawaii, is the U.S. Marine Corps component of the U.S. Pacific Command (PACOM). MARFORPAC provides operating forces to support Unified or Joint Task Force Commanders and Fleet Commanders in Chief (CINCs) in the Pacific Area of Responsibility (AOR). COMMARFORPAC serves as the principal adviser to the

Commander in Chief, CINCPAC on Marine Corps matters. He is responsible for organizing, training, and equipping forces for employment as directed by CINCPAC.[5]

3. Marine Expeditionary Forces

The Marine Expeditionary Forces (MEFs) are the largest of the task-organized expeditionary forces known as the Marine Air Ground Task Force (MAGTF). A MEF is comprised of a Marine Division, Air Wing, and Force Service Support Group, with approximately 45,000 Marines and sailors. Subordinate to the MEFs is the Marine Expeditionary Unit (MEUs). MEUs deploy aboard amphibious ships and provide a global forward presence.

There are three active-duty MEFs in the Marine Corps, to include I MEF, II MEF, and III MEF. The following sections describe each.

a) I MEF

I MEF is located in Southern California at Camp Pendleton. I MEF is composed of the 1st Marine Division, 3rd Marine Aircraft Wing, the 1st Force Service Support Group, the 11th, 13th and 15th Marine Expeditionary Units, the 1st Surveillance, Reconnaissance and Intelligence Group, and a Headquarters and Service Company.

I MEF is tasked to achieve and maintain combat readiness of assigned forces, plan for and conduct contingency missions, amphibious and other missions as assigned by the commanding general, Fleet Marine Force, Pacific. I MEF is charged with developing standard operating procedures for all aspects of air-ground task force operations and for the promulgation and updating of contingency and general war plans.[6]

b) II MEF

II MEF is located at Camp Lejuene, North Carolina. II MEF is composed of the 2nd Marine Division, 2nd Marine Aircraft Wing, the 2nd Force Service Support Group, the 22nd, 24th, and 26th Marine Expeditionary Units, the 2nd Surveillance, Reconnaissance and Intelligence Group, and a Headquarters and Service Company. II MEF also provides forces for missions assigned by the commanding general, Fleet Marine Force, Atlantic.

c) III MEF

III MEF is located at Camp Courtney, Okinawa, Japan. III MEF is composed of the 3rd Marine Division, 1st Marine Aircraft Wing, 3rd Force Service Support Group, the 31 Marine Expeditionary Unit, and a Headquarters and Service Company.

III MEF is also tasked to achieve and maintain combat readiness of assigned forces, plan for and conduct contingency missions, amphibious and other missions as assigned by the commanding general, Fleet Marine Force, Pacific. Figure 2 depicts a typical organizational chart for a MEF.

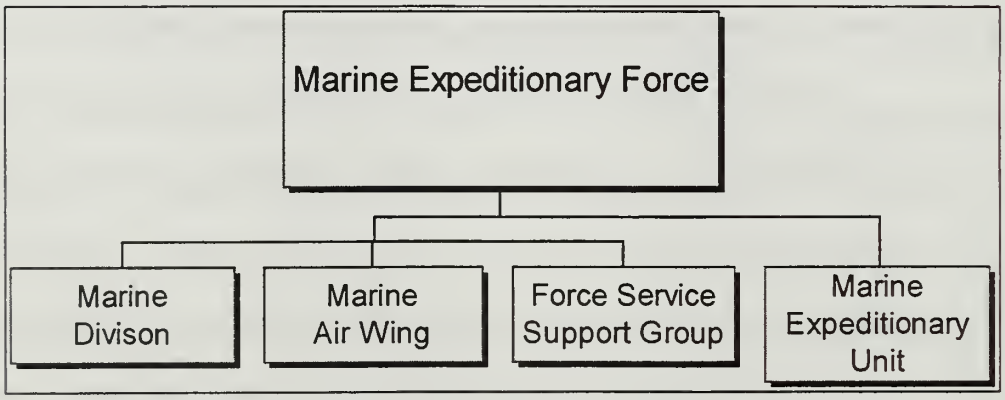

Figure 2. Typical Marine Expeditionary Force

Later in this paper, we describe how the MCEN applies to Battalion (BN), which is a subordinate element of the Division as depicted in Figure 3. This depiction is simplified to include only the major subordinate infantry units and does not include other units such as headquarters, artillery, light armored reconnaissance, engineer, or amphibious assault.

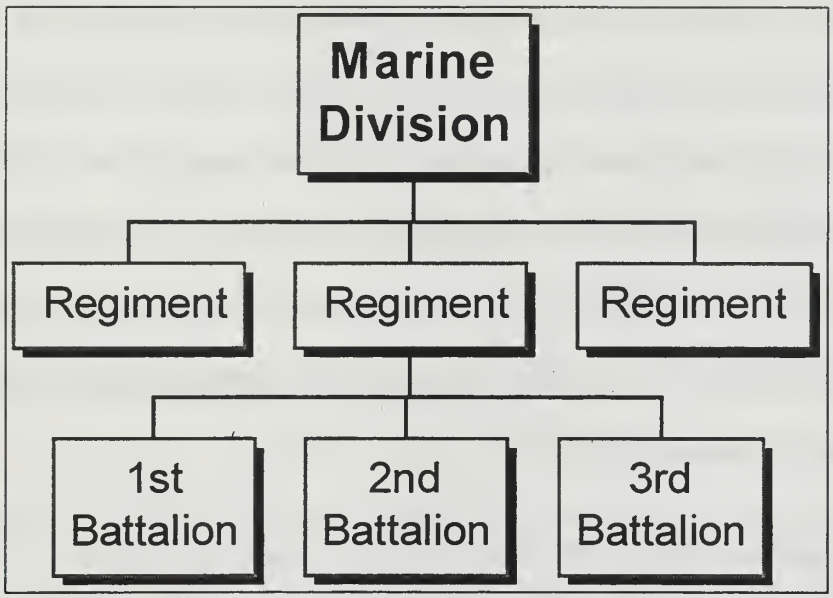

Figure 3. Typical Marine division organizational chart

4. Marine Forces, Reserve

Marine Forces Reserve (MARFORRES), located in New Orleans, Louisiana, is the Headquarters command for all the Marine Reservists and Reserve units located throughout the United States. MARFORRES provides policy, guidance, direction, and support to 104,000 Reserve Marines all across the United States.

MARFORRES is responsible for providing trained units and qualified individuals to be mobilized for active duty in time of war, national emergency or contingency

operations, and provides personnel and operational tempo relief for the active forces in peacetime.

5. Marine Corps Systems Command

Marine Corps Systems Command (MARCORSYSCOM) is located 35 miles south of Washington, D.C., aboard the Marine Corps Base, Quantico, Virginia. MARCORSYSCOM provides research, development, and acquisition of equipment, information systems, training systems, and weapon systems to satisfy all approved material requirements of the Marine Corps. The NOC is part of MARCORSYSCOM and is the focal point for network management. Its mission "...is to provide continuous, secure, global communications, and management of the Marine Corps Enterprise Network for Marine forces worldwide to affect information exchange across the Defense Information Infrastructure (DII)."[7]

B. MARINE CORPS ENTERPRISE NETWORK (MCEN)

To begin any discussion of the MCEN, it is imperative that we first define its structure. When used generically, an enterprise network is defined as "a complex network consisting of multiple servers and multiple domains over a large geographic area."[8] Therefore, the MCEN would include all of the servers and domains comprising the Marine Corps enterprise throughout the world. This includes all of the routers, switches, and servers, as well as the Secure IP Router Network (SIPRNET), and the Unclassified IP Router Network (NIPRNET). We have however, limited our discussion in this paper to the MCEN as it applies to use of the NIPRNET.

C. CURRENT ENVIRONMENT

1. Network Operating System

The MCEN is primarily a Banyan Vines-based NOS operating on Banyan Vines servers. While Banyan Vines servers and Cisco routers continue to dominate the Wide Area Network (WAN) environment, Windows NT servers constitute a fast growing population at the Local Area Network (LAN) level. It is at the LAN level of the MCEN where the migration from Banyan Vines to Windows NT NOS is occurring most rapidly. Banyan Vines servers are interconnected via Banyan's Street Talk Directory Service. Banyan Vines NOS and the Street Talk Directory Assistance service has been at the core of the Marine Corps' LAN/WAN.

Several different versions of Banyan are currently in use, including Banyan Vines versions 5.54, 6.2, 6.3, 6.4, 7.1, and 8.5. Version 8.5, to be released in October of 1998, is Y2K compliant. Since the migration to Windows NT will not be completed before the year 2000, all servers will need to be upgraded to version 8.5 before the year 2000.

2. Routers

The USMC WAN backbone is connected to routers at major Marine Corps bases and commands. The USMC WAN uses a series of dynamic routing protocols in order to pass native IP traffic between bases.

The following map depicts the location of the USMC's WAN routers.

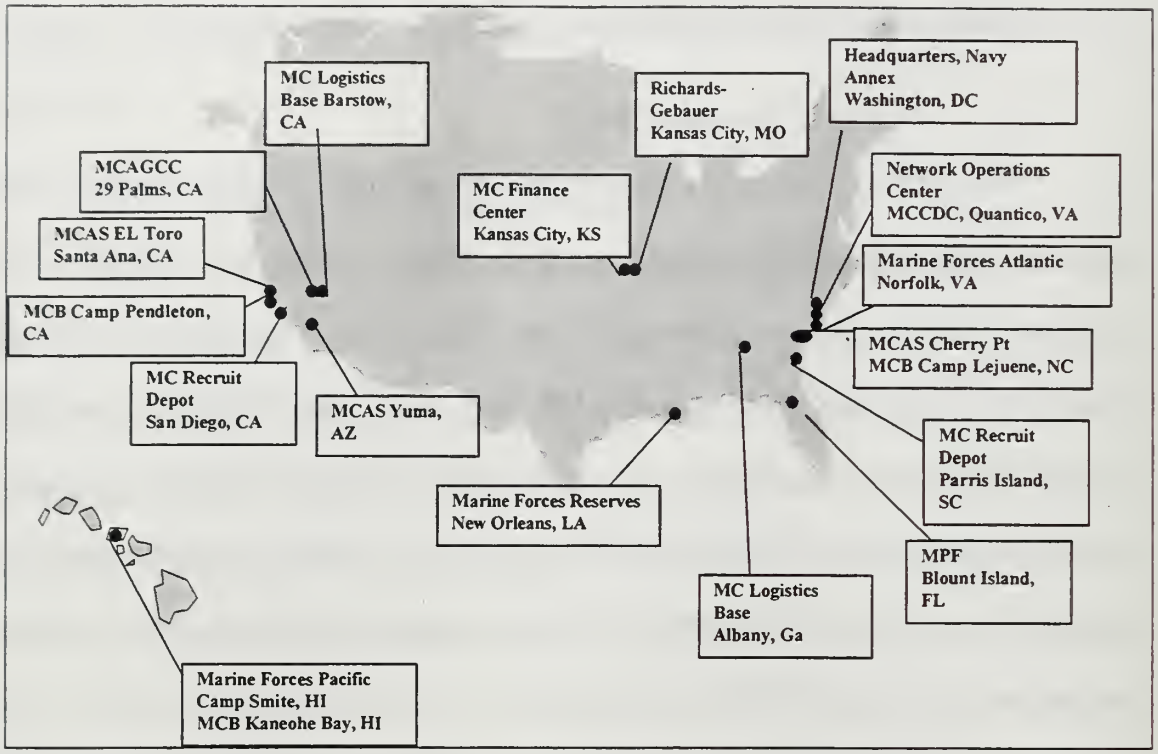
MC Logistics Base Barstow, CA
MCAGCC 29 Palms, CA
MCAS EL Toro Santa Ana, CA
MCB Camp Pendleton, CA
MC Recruit Depot San Diego, CA
MCAS Yuma, AZ
Richards-Gebauer Kansas City, MO
MC Finance Center Kansas City, KS
Headquarters, Navy Annex Washington, DC
Network Operations Center MCCDC, Quantico, VA
Marine Forces Atlantic Norfolk, VA
MCAS Cherry Pt MCB Camp Lejuene, NC
MC Recruit Depot Parris Island, SC
MPF Blount Island, FL
MC Logistics Base Albany, Ga
Marine Forces Reserves New Orleans, LA
Marine Forces Pacific Camp Smite, HI MCB Kaneohe Bay, HI

Figure 4. WAN router sites

3. Messaging

Banyan's Intelligent Messaging software is deployed as the predominant interpersonal messaging program used throughout the MCEN. However, due to the limited functionality and DOS-like characteristics of Banyan Vines mail, many users have begun substituting other mail programs for interpersonal messaging. The use of programs such as Happy Mail and Eudora Light have proliferated throughout the MCEN partially due to their Windows Graphical User Interface (GUI) capability. Moreover, these E-mail programs incorporate built-in features such as a spell checker, a file viewer for seeing the contents of attached files, and the ability to manually move E-mail messages from an inbox to other user-defined folders. Since not all MCEN computers

can support GUI E-mail programs, support for DOS-based E-mail will still be required in the near future.

4. Directory Services

The primary directory service in use in the USMC is Banyan Vines Street Talk Directory Assistant (STDA).[7] STDA services update all information within a "region" on an automated schedule of collection and rebuilds. Directory information gathered by Street Talk is gathered and shared by the Network Operations Center, which also adds other external entries or *inclusions* into the directory information prior to redistributing the Directory to the Marine Corps. These external names consist of mainframe inclusion entries and other addresses such as Lotus Notes mail and SMTP addresses. Migration to Microsoft's Exchange directory services is anticipated.

5. User Desktop

Desktop computers within the MCEN consist of a variety of processors, ranging from 286/386 up to the most modern Pentium II processors. These computers running a mixture of operating systems such as Windows 3.1, Windows for Workgroups, Windows 95, and most recently Windows 98. The older pre-Pentium desktop computers present the greatest challenge to the MCEN migration, as many are incapable of supporting current or future desktop application suites. However, since many of these computers are mission-essential, the need to support these systems will continue.

6. Remote Access

For those users not connecting to the MCEN via a LAN, Banyan dial-in service accounts provide the primary means of remote access. Banyan dial-in service includes mail, file, and print services to the dial-in user. Banyan's Intraconnect Server and Banyan Vines servers with LAN IP enabled provide additional means of remote access.

Windows NT's Remote Access Server (RAS) provides remote access capability for those commands employing Windows NT servers. Windows NT RAS can be configured to tunnel Vines services to the remote user.

7. 3270-Based Mainframe Access

Mainframe access is attained through a combination of both 3270 client software and the use of dumb terminals. Banyan 3270 (the entire collection of terminals and printers that communicate with a mainframe computer through the "3270" series controllers) is the predominant means of connectivity. The 3270 series controllers connect to the mainframe "locally" via an I/O channel or "remotely" via a synchronous (SNA-SDLC) serial link.

Mainframe access is rapidly shifting towards TN3270 services. TN3270 enables a standard ASCII terminal to emulate a 3278 terminal and access an IBM host across an IP network. TN3270E allows PC users on a TCP/IP network to log into an IBM mainframe that is running the MVS or VM operating system and supports the TN3270 protocol.

To run TN3270 services requires use of at least an IBM PC XT/AT, PS/2 or compatible system and 386/486 or Pentium-based processor with at least 640KB of

RAM. The limitation of TN3270 services has been due to the lack of SNA printer support, but that is being overcome by migration to the TN3270E standard currently being tested within the MCEN.

8. Legacy Services

Numerous legacy applications exist within the MCEN. Prior to the adoption of Microsoft Office as the Office Suite standard, numerous applications were being utilized throughout the Marine Corps, including Lotus Smartsuite, Wordperfect, Enable, and Harvard Graphics, to name but a few. These legacy applications, which include use of local databases and spreadsheets, will need to be migrated over either by porting (converting to Microsoft Office product standards) or re-hosting (moving onto web or Exchange Public folders, etc.).

9. Lotus Notes

A *Note* is an integrated client that offers functionality beyond that of a browser. Notes extend browser capabilities while adding access to integrated services, such as off-line support, so that parts of the intranet can be taken "on the road" and then re-synchronized with the office. Other services include full text search across multiple applications. Users can access their business productivity applications like SmartSuite and Microsoft Office directly from Notes. The basic browser can send and receive messages and view Web pages. The Notes client provides additional functionality, such as:

- Check spelling of e-mail messages

- View attached documents without having to detach them and load the application
- Create bulleted or numbered lists in an e-mail message
- Digitally sign messages
- Track edited messages by using a different color and font
- View the calendars of other users
- Convert mail messages into calendar entries
- View WEB pages while not connected
- Forward WEB pages to colleagues
- Review and edit documents while not connected
- Synchronize calendar with hand-held PDA devices such as a Palm Pilot
- Provide integration with SmartSuite or Office applications

The USMC Lotus Notes network is comprised of multiple domains, primarily the USMC and the Marine Corps Reserve Forces (MARFORRES) domains. The USMC domain has approximately 192 Notes servers. The primary operating system for the Notes network is Windows NT. Users can access the Lotus Notes servers through the MCEN.

D. MIGRATING THE MCEN

In November 1997, the Marine Corps undertook an effort to develop a migration document for the MCEN. The goal was to complete the document in preparation for the Technical Working Group meeting in January 1998. Marine personnel from the NOC met with Microsoft Corporation engineers, Microsoft Consulting Services engineers, and

third party software and hardware vendors for a series of technical discussions, product reviews, and white-boarding.

In May 1998, the NOC completed a technical discussion paper entitled *USMC Unclassified NT NOS/Exchange Messaging Migration.*[9] This document outlines a migration strategy for transitioning from the Banyan Vines NOS to Windows NT. It further identifies the need to begin planning for the eventual migration to NT 5.0.

E. SUMMARY

This chapter provided a brief description of the organization of the Marine Corps and the location of major commands. Additionally, the MCEN architecture was presented, along with current efforts to upgrade the NOS from Banyan Vines to NT 4.0.

III. TECHNICAL DEVELOPMENTS

Through the introduction of NT 5.0, Microsoft is trying to build on the momentum NT 4.0 has garnered in the marketplace. Figure 5 represents recent market studies that show that NT has passed Novell Netware as the network operating system with the largest installed base.*

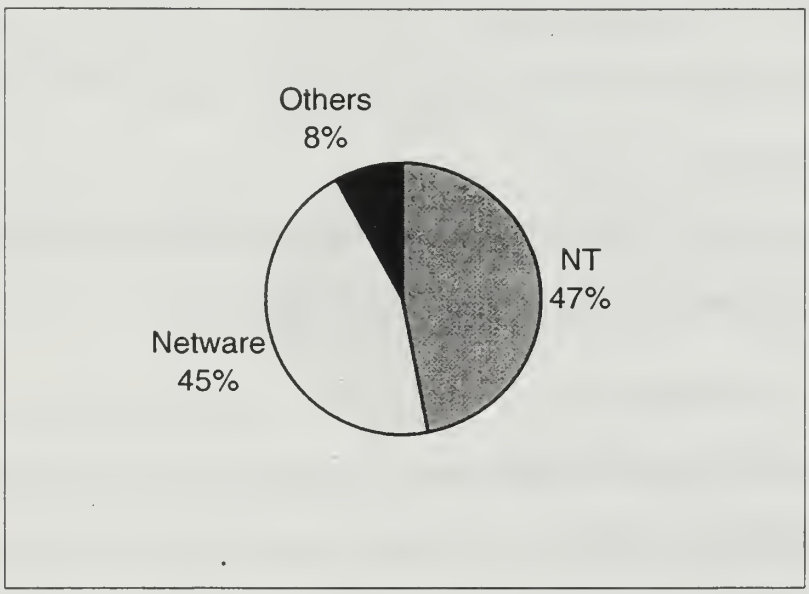

Figure 5. NOS Market Base[10]

While it is generally acknowledged that NT 4.0 has several disadvantages as compared to other leading network operating systems, NT 5.0 tries to do everything expected of a scalable and stable Network Operating System (NOS). This includes minimizing administrative overhead and total cost of ownership. To that end, Microsoft

* The same study interviewed 5000 network administrators who said they will choose NT over Netware as their next NOS by a ratio of 3:1.

has incorporated numerous new features into NT 5.0 that significantly increase system capabilities and stability.

This chapter will provide a brief technical explanation of several new NT capabilities that directly affect the management, administration, and operations of the MCEN. This chapter will not compare these features against other vendor products since the business decision to implement NT as the enterprise network systems has already been made. It is beyond the scope of this thesis to cover all of the new aspects and capabilities contained in NT 5.0. The authors will leave many NT innovations for future analysis and study.*

Several new features offering significant operational and administrative impact are presented in the following sections. These features are:

- Active Directory
- NT File System Version 5
- Kerberos Security

A. ACTIVE DIRECTORY

The Active Directory technology of NT 5.0 is the foundation for the entire operating system.[11] The Active Directory incorporates many of the functions previously offered by the NT 4.0 system databases and presents additional capabilities. It provides a unified platform to manage NOS resources by storing user information, network shares,

---

* The authors learned of many of the features discussed in this paper through Microsoft documentation and industry publications that focus on Windows/Intel products. The NT 5.0 Beta 1 release notes that accompany the NT 5.0 Beta software mention many capabilities that will be implemented in later beta releases or in the initial retail version.

policies, Domain Name Service (DNS) records and more.[12] Figure 6 summarizes how Active Directory interacts with all network resources.

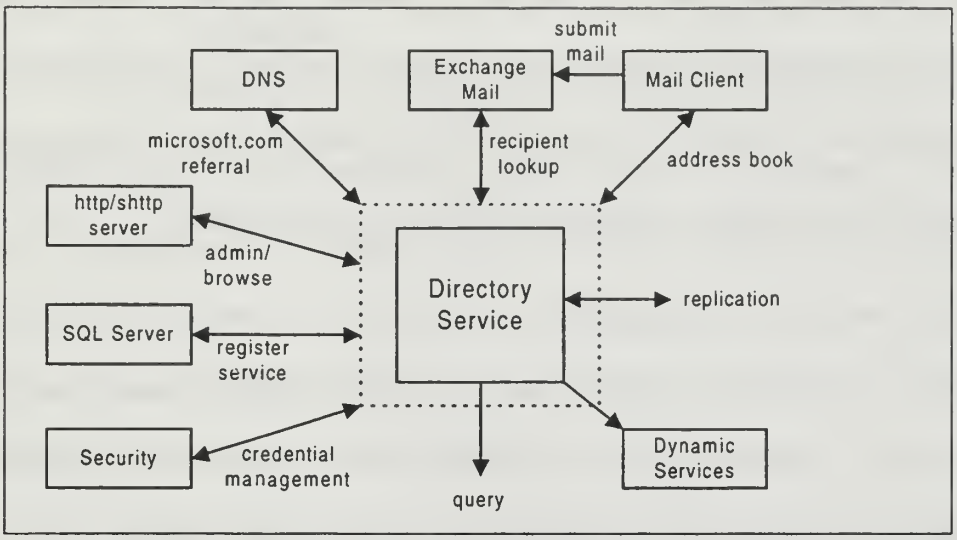

Figure 6. The Active Directory service interacts with all other network services.[13]

1. NT 4.0 Databases

NT 4.0 maintains several databases to track information about network users and resources. Two widely used databases are the *security accounts database* and the *browse list*. Understanding how these databases interact with users and resources will help describe the new innovations found in the NT 5.0 Active Directory.

a) Security Account Database

When a user turns on a client computer, the Win32 subsystem of the NT operating system starts the WinLogon process before the logon dialog box even appears. The user then enters the appropriate *username* and corresponding *password* and the WinLogon process passes this information to the Security Accounts Manager (SAM).

The SAM is the NT process that queries the security accounts database and validates that the user is authorized to logon to the domain. If the username and password correctly match the stored information in the security database, the user is properly authenticated and an access token is generated. These tokens comprise the security identifiers for the user accounts, including all group memberships. Whenever the user attempts to access a resource, the access token determines the level of access granted.[14]

*b) **Browse List***

Whenever a domain user needs to find a network resource, they usually do not know its exact network name. Because NT 4.0 does not employ a network directory, users can use NT's *Network Neighborhood* to find available resources. The *browse list* is the database that supports the network neighborhood.

The master browser is the computer that maintains the browse list for the domain. Many times the Primary Domain Controller (PDC) assumes the role of master browser and periodically publishes a read-only copy of the browse list to designated backup browsers throughout the network. When a client requires a resource on the network (i.e., printer, file, or storage device), they contact the first available backup browser. The backup browser then issues a copy of the current browse list. When a change to the browse list is required, the master browser must make the change to the database and publish the revised browse list to every backup browser. The disadvantage to this system is the single point of failure at the computer maintaining the master browser. If that computer is not operational, then no changes to the browse list are

possible. While network clients can access the last published browse list, no changes are possible until the master browser is functional.

c) Limitations

These databases are not designed for scalable enterprise networks. Both have limitations supporting distributed networks with large numbers of network resources. The database that supports the SAM is limited to 40MB. Since there is only one security account database per domain, this size limit translates to about 40,000 user accounts maximum. Since the USMC has at least 175,000 active duty members, the MCEN user account needs exceed the capability of one NT 4.0 domain.

In addition to the user account limitation, these databases have several limitations when operating on a network that has remote connections or TCP/IP. MCEN connectivity depends on TCP/IP and NT 4.0 can not route TCP/IP broadcasts for browsing services. Every subnet that is separated by routers must have its own master browser and the PDC coordinates the multiple browse lists in the domain. This coordination increases traffic in a bandwidth-limited environment.

2. Directory Services

The network directory is a special repository that stores information about network objects. This information includes security permissions and network locations of all network resources to include users, printers, files, and applications. The directory also acts like a telephone book because it provides easy reference for all network objects.

Network directory services are essential to enterprise networking. These services rely on the network directory to integrate users, resources, and applications throughout the enterprise. The directory services add significant value to the enterprise by eliminating redundant user information and by automating business processes throughout the network.[15]

Active Directory is the directory service included with NT 5.0. Microsoft designed Active Directory to work with organizations of any size. This range includes networks with only several users to a large distributed enterprise with millions of resources. The Active Directory is designed to make it easier to navigate and manage the NT domain, as well as to provide a secure single point of logon for all network resources.[16]

NT 5.0 is incorporating many common industry standards into its operating system. While Active Directory is not a true X.500 directory, it relies on the Lightweight Directory Access Protocol (LDAP) as its core protocol. LDAP (RFC 1777) was designed to provide X.500 capability with less information overhead. Active Directory uses the LDAP standard to provide a general-purpose directory for NOS specific directory services, as well as application oriented directory functions. Additionally, objects within the directory use the Internet Domain Name System (DNS) to identify themselves to other domain resources and systems.

The Active Directory includes the following capabilities:[13]

- Support for open standards to facilitate cross-platform directory services, including support for the Domain Name System (DNS) and support for standard protocols, such as LDAP and HTTP.

- Support for standard name formats to ensure ease of migration and ease of use.
- A rich set of APIs, which are easy to use for both the scripter and C/C++ programmer.
- Simple, intuitive administration through a simple hierarchical domain structure and the use of drag-and-drop administration.
- Directory object extensibility via an extensible schema.
- Fast lookup and Internet publishing via the global catalog.
- Speedy, convenient updates through multi-master replication.
- Support for services that have a short life span such as chat services, IP telephony, as well as other conferencing services.
- Backward compatibility with previous versions of the Windows NT operating system.
- Interoperability with NetWare environments.

Active Directory allows a more flexible and scalable organization of network resources and domains. NT 5.0 no longer implements the "hierarchy of servers" scheme found in NT 4.0 (PDCs and BDCs), but instead makes all Domain Controllers (DCs) peers with each other. Every DC maintains its own directory database and is equally capable of serving client requests for directory services. When a change is made to the directory database at one DC, the change is propagated to all other DCs. Large organizations with many domains can connect all their domains together using a domain tree structure. The domain tree provides a simplified trust relationship that allows cross-domain access for user accounts and network resources. If domain administrators wish to divide their domain along physical or functional lines, they can create a hierarchy of

Organizational Units (OUs), each with an OU administrator. This allows the domain administrator to focus on enterprise maintenance, rather than wasting time on routine tasks.

3. Active Directory Features

IT decision makers throughout the MCEN will have to evaluate their local organization and decide what Active Directory features are required for enterprise functionality and which can add value to their existing business practices. These new capabilities provide each organization an opportunity to evaluate their current state and decide if they should re-configure the network to optimize Active Directory. Specific Active Directory features that affect how MCEN administrators will manage their enterprise networks are listed below and then described in the following subsections:

- DNS integration
- Object naming
- Global Catalog
- Multimaster Replication
- Domain Trees
- Sites

a) DNS Integration

The Active Directory uses the Internet naming scheme (DNS) as its locator service. NT 5.0 resource names are the same as DNS names as illustrated in Figure 7:

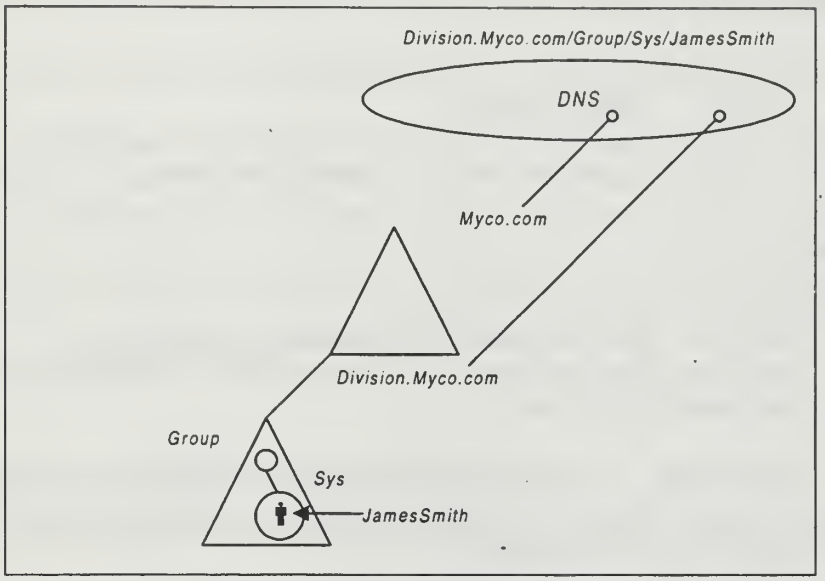

Figure 7. DNS is the Windows NT Locator Service[16]

For example, James Smith holds a user account in the "Sys" Group of the domain "Division" which belongs to the larger tree "Myco". James' email address might be smithj@myco.com. His user name would be the same as his email since DNS naming scheme is used by Myco. A HP printer assigned to the Sys department would be named HP2@Division.Myco.com and would be known to all domain tree users by that unique DNS.

NT 5.0 has the capability to dynamically assign client computers their TCP/IP address at startup using the Dynamic Host Configuration Protocol (DHCP). Once an IP address is assigned, the clients then register their DNS names and IP

addresses with a Windows Internet Naming Service (WINS) server in the domain. Whenever a client needs to resolve a name for a domain resource, the request goes to the WINS server who then returns the appropriate IP address. Eventually, Microsoft hopes to eliminate the proprietary WINS server and use a *Dynamic DNS* scheme based on approved Internet standards.

b) Object Naming

NT 5.0 provides several naming conventions to reference available resources:

- RFC822. These names are in the common email form of *someobject@somedomain.* Any object in the Active Directory can be displayed in this form.
- HTTP/URL. To provide easier access from WEB browsers, NT 5.0 allows URL path references to domain resources. HTTP://somedomain/path-to-object is an example URL.
- LDAP. Based on the X.500 naming convention, LDAP names are commonly used by Active Directory. These names are not intuitively obvious and the X.500 specifications are required to reference the named object.
- UNC. To provide backward compatibility with older Windows products, NT 5.0 supports the Universal Naming Convention (UNC).

c) Global Catalog

The Global Catalog is designed to allow users to find objects in other domains within the same domain tree. The Global Catalog is built automatically by the Active Directory replication system. While the attributes for each object stored in the Global Catalog are predefined by Microsoft, administrators can tailor these attributes to fit their own organizational needs.

A common use for the Global Catalog would be to provide a comprehensive address book of all the users in the organization regardless of where their domain resides in the tree. Users need only search for objects based on selected attributes and the Active Directory will search the Global Catalog if the resource is not found locally. All objects have at least one attribute stored in the Global Catalog for quick reference. This catalog is not as comprehensive as the directories held by each domain controller, but is instead comprised of a *partial replication* of each domain database. This reduced database allows many common queries to be resolved without communicating with the source domain. This design works well when domains in the tree are separated by remote links.

d) Multimaster Replication

NT 5.0 defines *multimaster replication* as the process of reproducing and synchronizing all directory information in the Active Directory of a domain. This distributed aspect of Active Directory is designed to optimize the anticipated query-to-update ratio. Because every domain controller has a complete Active Directory database, updates on one controller must quickly pass to all the other controllers in the domain. However, Microsoft expects as many as 99 directory queries for every single update and is therefore more concerned about resolving queries than about increased traffic due to updates.[16]

To properly replicate updates throughout the domain, NT 5.0 uses *Update Sequence Numbers* (USNs). Every property of every object has its own USN. Whenever changes are made to a property of an object, the USN is increased by one. Domain

controllers monitor each other for recent changes and request only those changes to bring their USNs up to date. If a domain controller receives two changes to the same property from two separate sources, an imbedded time-stamp is used as a tiebreaker. By using the USN scheme and not time-stamps as the primary update, perfect time synchronization is not critical for domain replication and consistency.

e) Domain Trees

Different domains within an organization join together to form a single domain tree. While a single domain can hold up to 10 million objects, domain trees allow for even greater scalability. When joining domains to a domain tree, administrators must maintain the DNS naming scheme implemented by the chain of command. Any child domains of a parent domain in a tree must inherent their DNS name as a suffix. Additionally, within domains, administrators can establish Organization Units (OUs) to delegate administrative control and to group resources and users for easier management. Figure 8 and illustrates the DNS inheritance requirements of child domain names and Figure 9 shows the hierarchy within those domains:

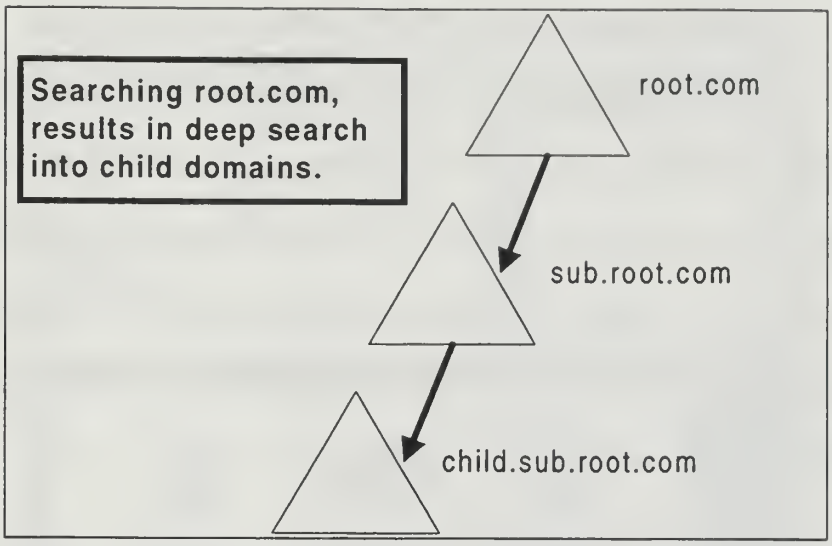

Figure 8. Child domains inherit their parent's DNS name.[16]

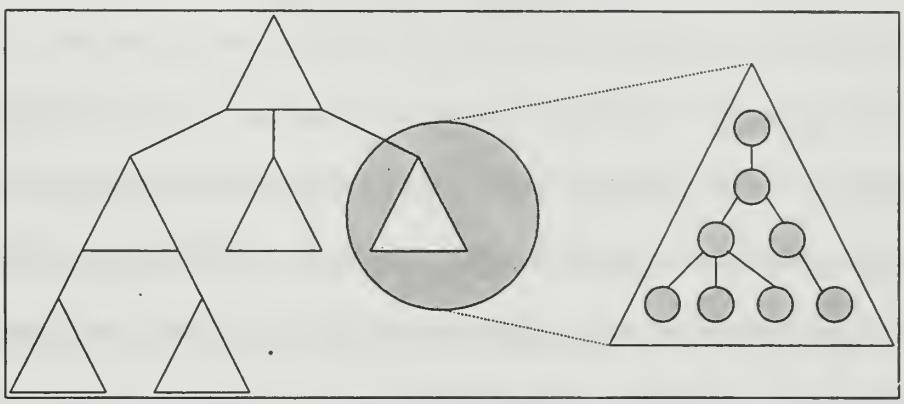

Figure 9. Active Directory uses a hierarchy of domain trees, domains, and OUs.

NT 5.0 extends the tree hierarchy up one more level to that of a *forest*. A forest is a set of several trees that do not share the same DNS name but do share a common global catalog. All trees in a forest share the same security configuration and continue the single sign-on concept. The Department of the Navy might find it beneficial to set up a forest that holds both Navy trees and USMC trees. While each service has its own DNS names, the forest allows users to work in either tree.

f) Sites

NT 5.0 administrators can use *sites* to efficiently configure their network. A site is defined as one or more TCP/IP subnets, and it allows for the physical grouping of Active Directory servers in a network. This provides mobile clients the ability to jump onto the network and logon to the closest domain controller as defined by their current site. This reduces the traffic between subnets and gives the administrator flexibility in designing network topology.

4. Microsoft Management Console

Microsoft Management Console (MMC) is a network server component that provides a common framework for all network administration programs. MMC acts as the user interface to the Active Directory and displays a window that hosts ActiveX objects (*snap-ins)* to administer parts of the network. Different snap-ins are organized into a tree structure much like Windows Explorer. MMC provides all the tools and information an administrator may need to complete various tasks and reduces the amount of time spent in the registry. Figure 10 shows how separate windows in the console display different views for each task:

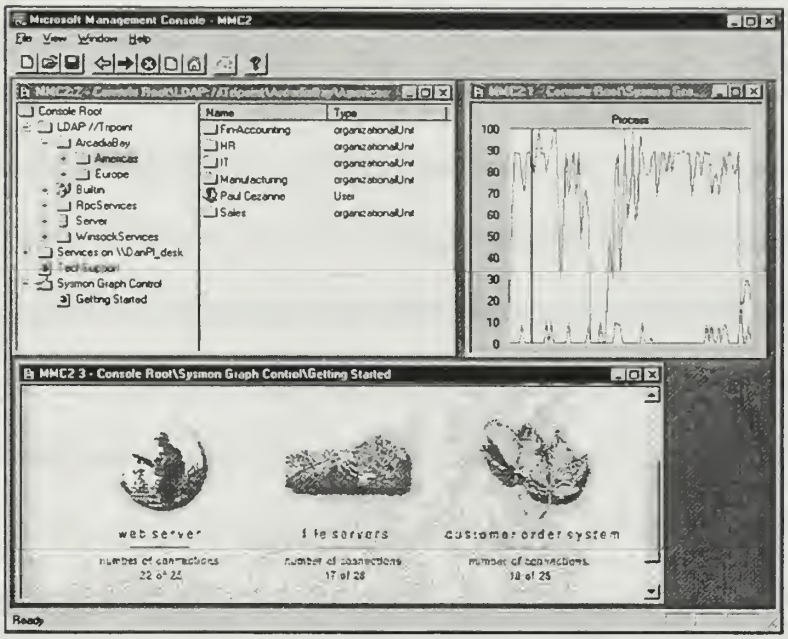

Figure 10. The MMC tool.[17]

B. NTFS 5

Windows NT 5.0 adds enhancements to the NTFS file system that are not found in NT 4.0. The new version of NTFS (NTFS 5) includes more robust disk volume management, better off-line storage and file encryption. To take advantage of the new NTFS capabilities, existing volumes will have to be manually upgraded to the new NTFS version. While the authors confirmed that NTFS 5 is backward compatible with NT 4 and WIN 95 clients, it does not support duel boot environments where other system volumes are not NTFS 5.

1. Volume Management

Two storage types are available in NT 5.0; *basic storage* and *dynamic storage*. The administrator configures volumes through the familiar Disk Management tool, with a few new options added in the new release.

Since NT 5.0 accommodates both basic and dynamic storage, a hard drive disk system can contain any combination of storage types. However, all volumes on the same disk must use the same storage type. Unfortunately, Beta 1 does not support a bootable dynamic disk. Therefore, a basic disk with system and boot partitions is required to implement NT 5.0. Since most MCEN servers will be NT 4.0 upgrades, the basic disk will be the default configuration for most situations.

a) Basic storage

Basic storage is supported by all versions of Windows, MS-DOS, and Windows NT. This is how the NT 4.0 disks are configured before the upgrade. When a disk is initialized for basic storage, it can hold primary partitions, extended partitions, and logical drives.

b) Dynamic storage

Dynamic storage is the other configuration option for disks supported by Windows NT 5.0. A disk initialized for dynamic storage can hold simple volumes, spanned volumes, mirrored volumes, striped volumes, and RAID-5 volumes. Dynamic storage allows the administrator to perform disk and volume management without having to reboot the operating system.

2. Quota Support

Assigning limits to the amount of storage space that each user can consume is an essential feature missing in NT 4.0. NTFS 5 allows the administrator to set limits by user depending on need. When the user exceeds the established limits, the system can either issue a warning or deny additional access. If MCEN administrators do not want to set quotas on users or groups, the quota feature can still be used to track how much disk space a certain user is occupying. This allows for flexible monitoring without restrictive practices.

Applications must abide by the same quota limits imposed on users. If an application tries to occupy more disk space then its privileges allow, then the disk will appear full and the application will act accordingly.

3. Hierarchical Storage Management (HSM)

HSM keeps track of files and applications that have been moved from *on-line* storage systems to secondary or remote *off-line* storage. HSM is particularly useful when a quota policy forces users with large file or application needs to store off-line. HSM relocates the files to alternate off-line storage such as optical media or magnetic tape and places a link in their place. This link points to the appropriate storage media and is transparent to the user. When the link is activated, it retrieves the file from the off-line repository or prompts administrators to load the media.

HSM allows a two-tier implementation based on the priority level of the stored data. For instance, the first tier could be reserved for a CD tower containing archived

files and the second tier would be a library of tape cartridges that require manual installation.

While this may sound labor intensive, it may work well for certain environments that have users with specialized needs. Many MCEN organizations may find that certain applications are seldom used and can be moved off-line to free space for current data. When a Marine deploys or goes on TAD, the administrator can move his files to storage but still have them available if required.

4. Security

NT 5.0 enhances the security of NTFS by implementing a built-in encryption option for data files. This built-in capability is called *Encrypting File System* (EFS). EFS has many advantages including greater security for attacks on the physical hard drive. NT *access permissions* are automatically assigned to every object by default, and they provide protection from remote network attacks but not from physical intrusion.

NT 4.0 has a physical vulnerability because several third party tools allow unauthorized users to boot a NT machine to a floppy disk then use utilities to scan the hard drive sector by sector. Any NTFS file not encrypted is thus vulnerable to attack. NT 5.0 tries to protect physical data through implementing EFS. The details of how EFS works are discussed later in the Security section.

Two scenarios where EFS capabilities provide valuable protection are:

- A stolen laptop – Laptops are particularly vulnerable because of their inherent mobility. EFS ensures that sensitive information can travel with the user without excessive risk.

- Unrestricted access – Office environments have different levels of physical security that may allow unauthorized access to the desktop machines.

C. SECURITY

The security model for NT 5.0 is distributed throughout the domain along with the Active Directory. The security information is no longer kept within the security accounts database, but instead it resides within the Active Directory. The global catalog allows single sign-on to the NT domain tree for each user anywhere in the enterprise network. All the privileges and resources available to a user in their home domain are available at all times.

NT 5.0 is designed to provide secure network services to not only other NT 5.0 server/workstations, but also to NT 4.0 server/workstations and WIN 95/98 clients. The security protocol used for compatibility with older Microsoft systems is NT Logon Manager (NTLM), although NT 5.0 also employs several additional security protocols for network services. The protocol designed to interact with Active Directory for routine network security is the Kerberos Version 5 protocol based on RFC 1510.[18]

1. Kerberos Authentication

Developed from a project at MIT, the Kerberos protocol has developed into a mature security standard. The Kerberos protocol is an improvement over NTLM in several ways, notably by eliminating unencrypted password transmission over the network. This is particularly valuable to the MCEN when remote clients have to dial-in to the server for access.

Kerberos relies on a three-sided, shared secret-key scheme to effect authentication. The three sides include the client, the server and a *key* database called the Key Distribution Center (KDC).[19] The KDC maintains the key information for all users in the domain and is considered a trusted third party in the NT security schema. The KDC establishes a realm for each domain and allows clients to authenticate with different servers in different realms.

NT 5.0 designates the domain controller as the KDC and the Active Directory maintains the key database. When clients log on to the network with their usernames and passwords, a Kerberos session begins that returns an authenticated *ticket* that is used throughout the Active Directory. NT 5.0 domains will trust any Kerberos ticket issued by another domain in the same tree. This forms transitive trust relationships that were not attainable in NT 4.0. Previously, the network administrator had to build one-on-one trust relationships with every domain in the enterprise. This resulted in N*(N-1) relations given N number of domains. Given the four domains shown Figure 11, we can easily determine the number of 1 to 1 relationships required, 4*(4-1) = 12.

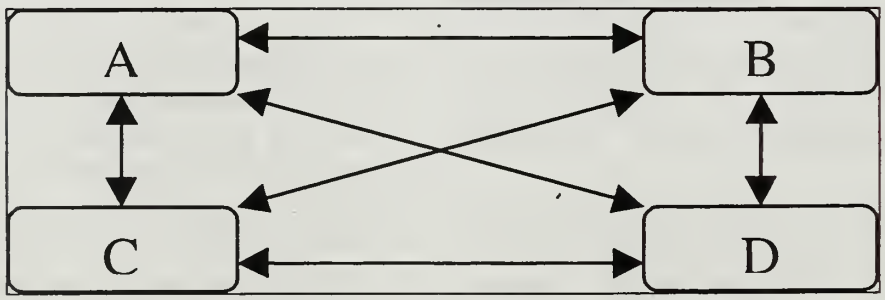

Figure 11. Numerous trust relationships are required in NT 4.0.

When the number of domains increase, the number of trust relationships quickly becomes unmanageable, however. Kerberos avoids this management puzzle by providing single logon transitive access throughout the domain tree. This greatly increases the enterprise functionality of NT 5.0. When a domain joins a tree, the Kerberos trust relationship is automatically established and no additional trust relationships are required among tree members. Additional flexibility is built into the Kerberos scheme that allows administrators to configure how long each ticket remains active. This time is called a *session* and it can be set according to the security environment of the organization. Figure 12 demonstrates that if domain A trusts domain B and domain B trusts domain C, then A trusts C:

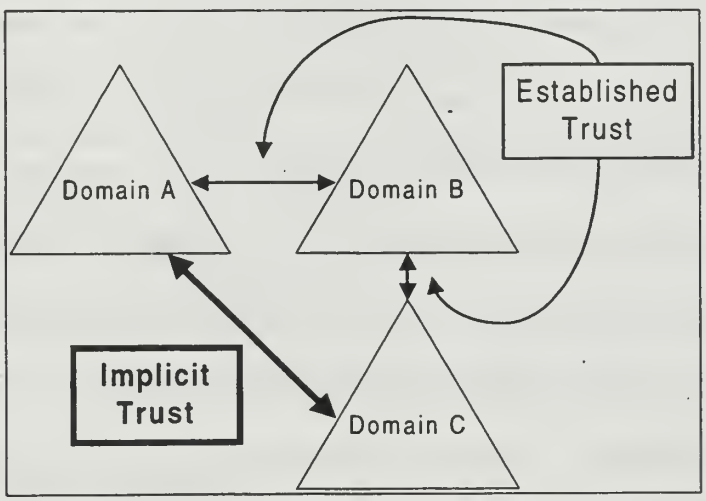

Figure 12. Domain in a tree share transitive trust relationships.

Since the Kerberos ticket returned to the user provides only identification information, NT continues to use the Security ID (SID) concept from NT 4.0. These SIDs create security access tokens that allow users to access system resources based on their Access Control List (ACL) settings in the directory. While the KDC and Kerberos

version 5 protocol is intended for heterogeneous implementation, non-NT KDCs will not be able to interpret the SIDs that accompany the client ticket. Microsoft intends to develop the logon process to allow authentication across different KDC varieties, such as UNIX.

2. Encrypted Files System (EFS)

EFS is based on the public key encryption architecture found in the Active Directory. The user can selectively decide which files (or which folders containing sets of files) to encrypt. Each encryption action generates a random key that is not based on the user's public/private key. This helps prevent deductive cryptanalysis attacks on the NT system.[20]

Since EFS operates at the NT Kernel level, encryption is transparent to the user. Once the encryption option is selected for a folder or file, all subsequent read/writes will automatically encrypt and decrypt as required. Any temporary files are likewise encrypted and NT keeps the sensitive keys out of the page file to prevent undue exposure.

The first version of EFS will use the standard 56-bit DES algorithm to generate keys. Future releases will allow alternative key algorithms that should provide stronger encryption capabilities. Additionally, file sharing will not be possible with the first release of EFS, but later versions will make us of the public key architecture to allow key exchange for file decryption.

D. HARDWARE

1. Server Components

NT 5.0 release notes recommend a minimum server hardware configuration considerably greater than NT 4.0 specifications. However, considering Moore's law (computer processing power doubles every eighteen months), the NT 5.0 minimum server standards are not hard to meet with current server configurations. Table 1 shows both the USMC and NT 5.0 minimum recommendations for server hardware:[3]

Hardware	USMC	NT 5.0
CPU	Dual 200 Mhz Pentium Pro	133 Mhz
Cache	512K	NA
RAM	256 MB	64 MB
Hard Drives	Two 4 GB SCSI	286 MB
Backup device	One 4/8 GB DAT Drive	NA
Removable storage	One floppy drive	3.5"
CD-ROM	6X SCSI	Any
Smart Card	Dual PCMCI card reader (Type II/Type III)	NA
Hard Drive Controllers	Two Ultra SCSI	NA
Monitor	VGA	VGA
Input device	Pointing device	Optional
Keyboard	Standard	Standard

Table 1. Minimum server hardware list.

2. Network Resources

The above table does not specify any standard for the network interface cards or for the connections to network peripherals and devices. NT 5.0 Beta 1 is missing support from common protocols such as 100BaseTX, but the retail version promises to include support for a wide range of modern network protocols.

Especially important to the MCEN is the capability for Asynchronous Transfer Mode (ATM). NT 5.0 provides two methods of ATM support, *ATM LAN Emulation* and *TCP/IP over ATM.*[21]

a) ATM LAN emulation

This mode provides generic support for most common network protocols such as ENTAIL, IPX/SPX and TCP/IP. More detailed information about LAN Emulation can be found in the NT 5.0 Release notes.

b) TCP/IP Direct support

Direct support for TCP/IP over ATM uses the ATM Address Resolution Protocol (ARP) and Multicast Address Resolution Service (MARS). ATM ARP and MARS allow the TCP/IP protocol stack to work directly over ATM media. These services also provide IP to ATM address resolution and IP multicast/broadcast for TCP/IP network clients.

When a computer with ATM services is upgraded to NT 5.0, ATM LAN emulation is installed by default. Since the MCEN uses TCP/IP as the primary network protocol, TCP/IP Direct support via ATM ARP/MARS is the preferred configuration.

E. SUMMARY

Microsoft incorporated many new changes into its latest NT version. While many of these updates are geared more towards the commercial sector, this chapter identifies several new NT 5.0 developments that directly affect the MCEN. Key features in NT 5.0 are:

- X.500 Directory Services
- NTFS version 5
- Enhanced Security

The benefits gained when implementing all three of the above capabilities provides a compelling reason for the MCEN to upgrade to NT 5.0.

IV. MIGRATION

A. OVERVIEW

This chapter emphasizes three critical areas in the migration process; (1) *preparing the environment; (2) executing the upgrade; and (3) MCEN implications.* The first area will propose several general actions Marine Corps Enterprise Network (MCEN) administrators can take to prepare their environment for an NT 5.0 upgrade, to include the evaluation of current policies and practices as well as the development of a recovery plan if the upgrade is not successful. The second area will describe possible upgrade configurations MCEN administrators may find and what problems the authors discovered with each scenario. Finally, the chapter will conclude with a discussion of significant migration implications for the MCEN.

1. Assumptions

To help illustrate the migration process, a standard infantry battalion will serve as an example of a generic unit participating in the MCEN. While the MCEN is actually comprised of several hundred units, each with their own NT 4.0 domain, this migration discussion will focus on the actions appropriate to one domain administrator. The authors chose an infantry battalion, as this unit typifies the Marine Corps at its lowest level of organizational command.

The fictitious battalion (1st BN) is structured as an organizational hierarchy as illustrated in Figure 13:

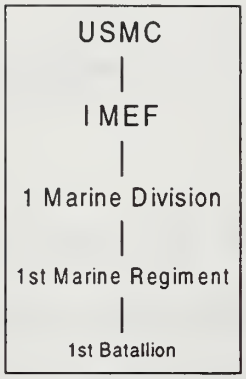

Figure 13. Organizational hierarchy

While several likely scenarios are presented as starting points for an upgrade, the authors make the assumption that MCEN servers will already be operating NT 4.0 and that earlier Network Operating Systems (NOS) versions have previously been removed from the networking environment.* Further, it is assumed that the servers will be operating as per the guidelines established in the NT 4.0 migration handbook published by C4I HQMC for the USMC.[3]

The computers used in migration testing by the authors to simulate MCEN Domain Controllers (DCs) represent a generic configuration as opposed to the most recent technology. Given the investment in current server technology, it is not realistic to assume that all NT upgrades will occur on brand new computers with the latest options. With this in mind, all NT 5.0 upgrade tests were conducted using a computer representing a typical "low-end" system.* The security level assumed for this environment is *Sensitive*

---

* For the purposes of this paper, the terms *NT server*, *MCEN server* or *server* refer to a physical computer running as a DC, not software running a server function.

* All references to NT 5.0 more specifically refer to Windows NT 5.0 Beta version 1 of May 1998. This reference is constant throughout the paper.

*but Not Classified.** This server configuration would support a standard battalion-sized unit operating in a physically controlled environment within a USMC base.

2. Configuration

Three different computers were used in testing. Two computers provided WIN 95 and NT 4.0 client functionality. The third computer acted as the server for all upgrade configurations and utilized the following hardware as shown in Table 2:

Hardware	Test PC
CPU	166 Mhz Pentium
Cache	256K
RAM	96 MB
Hard Drives	One 4 GB SCSI
Backup device	One 4/8 GB DAT Drive
Removable storage	One floppy drive
CD-ROM	8X SCSI
Smart Card	Dual PCMCI card reader (Type II/Type III)
Hard Drive Controllers	Two EIDE (SCSI adapter card installed)
Monitor	VGA
Input device	Pointing device
Keyboard	Standard

Table 2. Hardware configuration for test PC

B. PLANNING

For organizations undertaking the significant upgrade from NT 4.0 to 5.0, several preparatory steps will expedite the upgrade process and make better use of Active Directory features following the installation of NT 5.0. These steps include analyzing the current NT 4.0 environment and deciding what changes to make to facilitate the upgrade.

---

* Additional studies are required to investigate the additional implications of upgrading classified servers in a more vulnerable environment.

To that end, administrators should familiarize themselves with NT 5.0 by gathering all available documentation and guidance. Some initial steps are discussed in the following sections.

1. Domain model

The most common domain model in the MCEN is a *Single Domain*. A single domain will exist for each Major Supported Command, Base, Post, Station, Command Element, and deployed unit in the USMC.[3] Due to security considerations, domains may not extend beyond firewalls. Remote users may only connect to a domain through secure remote access services such as Point to Point Tunneling Protocol (PPTP).

The MCEN currently supports a decentralized enterprise by creating single domains throughout the USMC. Each domain has a local administrator who completely owns and maintains all domain resources. Only the local administrator can make necessary changes to the domain, however, organizations may have implemented trust relationships between domains so users can access resources in other domains. This results in complicated trust relationships that are commonly found in an NT 4.0 *complete trust* model. These trust relationships should be discontinued before any migration occurs as NT 5.0 will establish trusts based on Active Directory relationships within the domain tree. The single domain model offers the most straightforward migration starting point to NT 5.0. As such, if other domain models are used in the MCEN, they should be consolidated into a single domain if possible.

Another possible model in the MCEN is the master domain with a single resource domain. While this type of model is discouraged by HQMC, special circumstances may warrant this configuration. Figure 14 and Figure 15 display these two domain models:

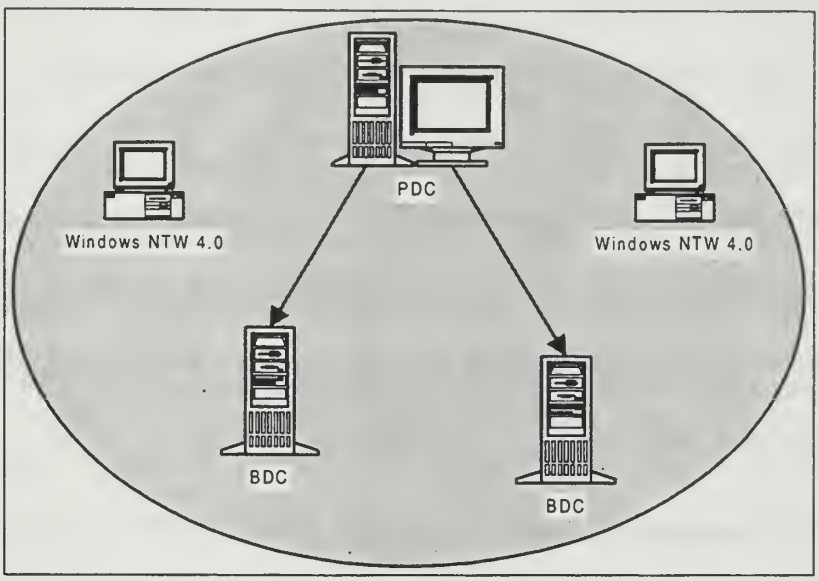

Figure 14. Single Domain[22]

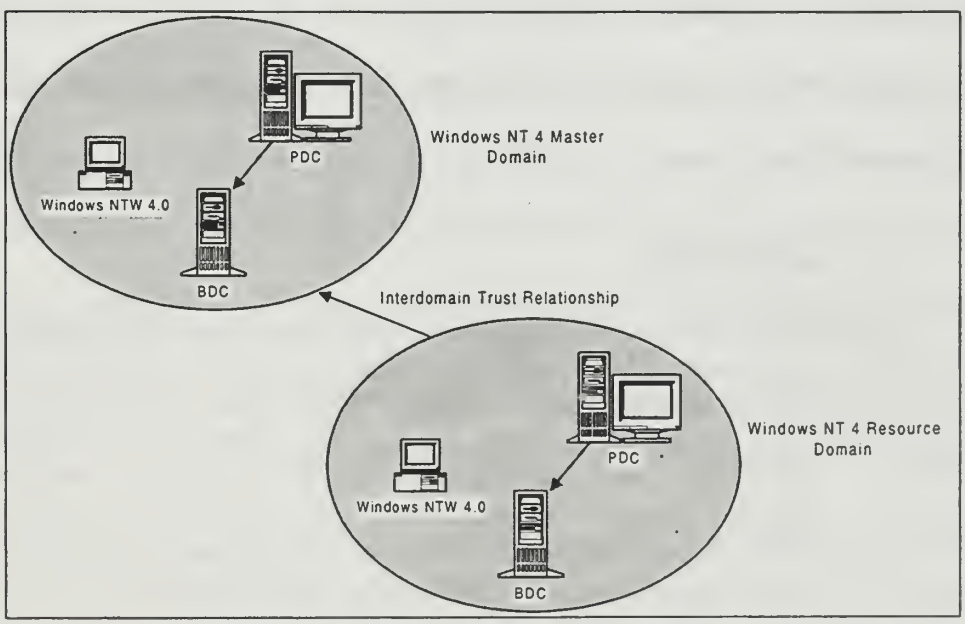

Figure 15. Master domain with resource domain[23]

Before MCEN administrators initiate any migration actions, they should attempt to deploy at least two Backup Domain Controllers (BDCs), in addition to the Primary Domain Controller (PDC), within the existing NT 4.0 domain. This will provide several levels of fault tolerance, to include one at the new NT 5.0 level and another at the old NT 4.0 level. If the migration is successful, the administrator will want to maintain at least two Active Directory DCs for redundant services in the event that one fails. Additionally, keeping a BDC running in NT 4.0 is a prudent step to guarantee a "failsafe" option if the PDC and first BDC do not upgrade correctly to NT 5.0. To re-establish a working environment, the administrator would promote the remaining BDC to a PDC and return the domain to NT 4.0.

2. TCP/IP

All domains in the MCEN should have TCP/IP implemented as their standard network protocol. The Microsoft proprietary protocol, NetBEUI, is a non-routable protocol and should not be used. Additionally, NT 5.0 relies heavily on the use of DHCP and Dynamic Domain Name Service (DNS) which requires TCP/IP support.

3. DHCP/WINS

NT administrators should implement Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS) in their domains before migrating to NT 5.0. DHCP will help identify any TCP/IP conflicts or problems as the administrator defines the applicable DHCP scopes and options. WINS will help with

backward compatibility when users operate in a mixed NT 4.0/5.0 environment. After the domain has fully migrated to NT 5.0, WINS is no longer required.

4. NT DNS Server

Planning for a Domain Name Service (DNS) environment will prevent many potential migration problems. While implementing an NT DNS server may not be appropriate for all organizations and their domains, evaluating the domain for DNS compatibility is a required action. As discussed in the previous chapter, NT 5.0 uses DNS, not NetBIOS, as the naming scheme to locate Active Directory resources. NT 4.0 uses the NetBIOS naming convention which allows a greater range of natural name variations than NT 5.0, but it is not DNS compatible. Since NT 5.0 adds all parent domains to the end of the local domain name (i.e., noc.hqmc.usmc.mil) administrators should verify that existing domain names are DNS compliant. DNS naming rules allow only the following characters: A-Z, a-z, 0-9, and "-" (no underscoring or spaces allowed). If problematic resource names are changed to DNS names before migration, many problems will be avoided.[24]

Additionally, MCEN administrators should confirm the DNS name for their domain by coordinating with appropriate senior organizations that will become parent domains in the NT 5.0 naming scheme. In order for any child domain to join a domain tree and share Active Directory resources with the enterprise, NT 5.0 requires a valid DNS name for both the child and parent domain. If proper naming does not occur, the domain tree relationships are not established during migration and can not be added later.

Depending on the size of the unit implementing the NT upgrade, it may rely on DNS servers that reside in other domains. If this is the case, that DNS server must be available during the upgrade process and it must support *service locator record types* as defined by RFC 2052 (SRV records).[25] Dynamic DNS mapping is another valuable feature that should be incorporated into DNS services. While UNIX DNS servers can support SRV and Dynamic DNS, NT 5.0 DNS services are designed specifically for these functions. However, regardless of what DNS servers are available, the administrator should set up an additional NT server in that local domain that will also participate in the migration to NT 5.0. This will allow DNS redundancy if required and thus ensure Active Directory compatibility in the future.

5. Determine NT 5.0 Configuration

The administrator can migrate the existing NT 4.0 domain and associated servers several different ways. The proper approach to upgrading the domains and servers depends on their roles before and after the upgrade.

a) Determine Domain tree configuration

Any NT 4.0 domain can evolve into an NT 5.0 domain via the three different migration methods. Each method will place the upgraded domain at a different level of the MCEN domain tree depending on the upgrade path. The three migration paths are:

- Create a new NT 5.0 domain and create a new domain tree
- Create a new NT 5.0 domain and join an existing domain tree

- Merge into an existing NT 5.0 domain

The proper migration method depends on where the current NT 4.0 domain currently exists in the MCEN and where the administrators want their domain to reside relative to other domains. An effective method for determining which of the three upgrade methods applies is to examine the DNS name that the NT 5.0 domain will use. The MCEN should only have one upgrade that creates a new domain tree. This would be the root domain *usmc.mil.*[*] All other domains will join existing child domains or create new ones.

If the MCEN organization has a parent in the DNS name, then the domain must join the appropriate tree under the assigned parent. For example, if HQMC were to have a DNS name of *hqmc.usmc.mil*, then the administrators at HQMC would have to join the tree just below their parent domain. In this case, the parent would be the USMC root domain *usmc.mil*, which is the top-level domain in the MCEN. Any other child domain that fall within the HQMC organization, such as a domain for the NOC, would also join the *USMC* tree below their parent *hqmc.usmc.mil* domain.

b) Determine Server Types

While NT 4.0 presented the user with a choice of three server types on installation, NT 5.0 only has two: the *Domain Controller* and the *Stand-Alone*. This is

---

[*] If this domain does not exist in NT 4.0, then it would need to be created with a new NT 5.0 installation before any other organizations could upgrade. Once an NT 5.0 domain is created, it may move around within a tree but it may not join a different tree.

because NT 5.0 no longer differentiates between DCs. The administrator must decide which server type is appropriate for each situation.

(1) Domain Controller (DC). There are three basic alternative configurations for DCs whenever a server is migrated to NT 5.0. These choices are very similar to the domain choices previously listed.

- First DC in the top-level domain of a tree
- First DC of a child domain
- Replica DC in existing domain

The very first DC the MCEN upgrades in the enterprise should be the PDC of the top-level domain. This domain would assume the root DNS name of *usmc.mil*. Every other organization in the MCEN will upgrade their first DC in a child domain. When a second DC in any domain is upgraded, it will be a replica of the first. This holds true for the top domain and all child domains.

(2) Stand-Alone. Stand-Alone servers exist in NT 4.0 as well as NT 5.0. This type of upgrade is very straightforward and the administrator can upgrade the server any time after the Active Directory is established.

6. DCs

When an NT 4.0 domain is migrated to NT 5.0, the administrator should always update the PDC before any NT 4.0 BDC. By upgrading the PDC first, the domain can immediately join an existing domain tree with the respective parent domains, thus

allowing the administrator to start using Active Directory tools as soon as possible.[23] Because NT 5.0 supports mixed environments, the upgraded DC will appear to be a PDC to legacy NT 4.0 systems and an NT 5.0 DC to all Active Directory resources within the domain tree.

Since the Primary DC (PDC) will be the first DC to receive the NT 5.0 upgrade, an emergency action plan is required in case of an aborted upgrade. While several methods are appropriate, one possible solution for restoring the NT 4.0 domain back to health after an aborted upgrade is to have a BDC in reserve. This means that a BDC with the latest copy of the security and browser databases is held in a "disconnected" standby mode during the upgrade process. In the event that the upgrade does not complete successfully, the administrator can quickly bring the BDC on-line and promote it to PDC status with no loss in domain functionality.

7. Third Party Influences

All administrators should review the latest NT 5.0 Release Notes contained within the installation disk for detailed information. Instructions on how to create NT 5.0 start-up and recovery disks, along with documentation detailing unsupported applications and hardware, are included. Generally, all virus-scanners, third party services or client software and UPS devices should be removed from the existing configuration. Additionally, NT services such as WINS or DHCP should be stopped to stabilize the server database prior to upgrade.

8. PC Lab

Administrators can create a test environment in order to practice NT 5.0 upgrades in a simulated environment by taking the following steps:

- Configure test NT 4.0 DCs and clients then run through several upgrade scenarios.
- If a network-monitoring tool is available, check the network traffic before and after the upgrade.
- Observe the interaction between clients in a mixed NT 4.0/5.0 environment and in an NT 5.0 exclusive environment.
- If possible, set up a computer as a new BDC on the existing NT 4.0 domain. Disconnect this BDC and move it to the Lab for the upgrade test.

Once the computer is in the lab and off the network, the administrator can promote the test BDC to a test PDC and practice the upgrade process. In order for the upgrade process to perform properly, Dynamic DNS services are required for the Active Directory. The administrator can also install NT 5.0 DNS services simultaneously with the DC upgrade and provide the necessary functionality.

9. MCEN Example

Assuming the 1st BN administrator followed the MCEN guidance on implementing NT 4.0, a Single Domain model is already in place. If instead 1st BN were running a Master Domain model, the network resources would migrate from the Resource Domain to the new NT 5.0 domain after upgrade. To start the process, the administrator in 1st BN follows the steps listed below:

- Gather available documentation on NT 5.0
- Assess current state of NT 4.0 domain

- Consolidate domains (as required)
- Implement TCP/IP with DHCP and WINS
- Conform to NT DNS naming scheme
- Determine NT 5.0 configuration
- Configure "Reserve" BDC
- Stop third party programs
- Rehearse upgrade in PC Lab

The 1st BN administrator then conducts a detailed review of current network conditions and realizes that some of the servers on the network still provide IPX/SPX and NetBEUI protocol service. After ensuring that TCP/IP is the only protocol on all domain servers, the administrator verifies that all possible network resources are using DHCP services to obtain their IP address, gateway address, WINS, and DNS information.

The next step is to coordinate with the network administrator at his next higher level of command and discuss the DNS naming scheme that will be used throughout the Regiment. Since 1st Marine Regiment will be 1st BN's parent domain, this is critical information. 1st BN also needs to know whether they must start their own DNS services or if they should rely on the Dynamic DNS service on Regiment's NT 5.0 server. The Regiment might suggest that 1st BN use the regimental DNS server for the short term since they have a high capacity network link between the two units. They could also emphasize that 1st BN should implement their own DNS server for deployments away from the Regiment. The two administrators finally agree on the appropriate domain

name for 1st BN based on the DNS guidance from the MCEN documentation: *1bn.1mar.1div.1mef.usmc.*

The administrator can now diagram the expected domain tree configuration and analyze the Kerberos trust relationships. The tree for 1st BN will look like Figure 16:

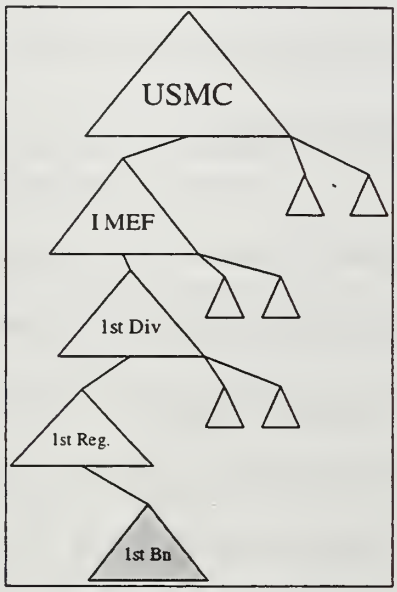

Figure 16. Joining a the MCEN domain tree

Armed with this knowledge, the battalion administrator knows that creating a new NT 5.0 child domain and joining an existing domain tree is the correct configuration. Additionally, information such as the address of the parent domain and the IP address of the nearest DNS server is also important. Before the upgrade begins, however, practicing the migration in a lab setting is essential.

C. EXECUTE THE UPGRADE

Most organizations in the MCEN will want to upgrade their PDCs to NT 5.0 before any other computer. This will provide an Active Directory environment for the

remaining NT 4.0 servers to join. NT 5.0 upgrade wizards recognize the NT 4.0 server role and will try to migrate that server accordingly. When upgrading a BDC, NT 5.0 assumes that a PDC was previously upgraded and makes the BDC search for the Active Directory resident on the existing NT 5.0 DC. If the BDC is the first to upgrade, NT 5.0 has problems during the installation. These problems are discussed in the BDC section below.

Once the administrator has completed all the planning steps and conducted a thorough system backup, the domain is ready for the upgrade to NT 5.0. The first step for all NT 5.0 migrations is to read the latest release notes that accompany the NT 5.0 CD-ROM. The notes will explain basic actions to take for the upgrade, to include shutting down many of the server services (i.e., DHCP/WINS, FTP, and DNS) and disabling any anti-virus programs. Once the latest guidance in the release notes is followed, the administrator may insert the CD-ROM and start the upgrade process.

NT 5.0 uses wizards to walk the administrator through the upgrade options, which helps to make the upgrade environment feel very familiar. The wizards ask a series of questions about the desired NT 5.0 configuration and then draw the rest of the basic information from the existing NT 4.0 system. Information such as computer name, IP address, and current driver specifications are imported from the NT 4.0 system.

1. NT 4.0 (Upgrade)

This migration demonstration starts with a server setup configured for a typical NT 4.0 domain as described in the USMC NT 4.0 discussion paper.[3] The hardware configuration is the same as listed in Table 1.

Most of the NT 5.0 installations will be conducted on a server already running NT 4.0. This type of installation is called an upgrade as opposed to an installation. NT 5.0 recognizes the original server settings and carries them forward into the new system. When necessary, NT 5.0 will prompt the administrator for inputs so appropriate features are implemented. The administrator must correctly answer the installation questions to avoid time-consuming configuration changes after the transition.

2. PDC

As noted above, the first DC to receive the upgrade in all migration configurations is the PDC. The PDC for this particular test was configured with basic services which did not include specialized file or application services.

a) Description of the PDC

Basic PDC services included DHCP, WINS, and other default NT services. FTP and DNS were not running on the PDC. The NT Boot partition that contained the NT system files consumed 188 MB of disk space. The computer name was *NT5BETADC* and the domain name was *NT5BETA*. The TCP/IP property window displayed the DNS information before migration. This property window listed the host as *NT5BETA* and DNS as *nps.navy.mil*.

b) Starting the upgrade

As soon as the NT 5.0 disk was inserted into the CD-ROM, the wizard popped up to recognize the NT 4.0 configuration. The wizard immediately offered to upgrade to NT 5.0. After selecting to upgrade, the wizard offered two upgrade choices:

(1) New Installation. This installs NT 5.0 alongside the existing NT 4.0 installation. It also creates a dual-boot environment where the administrator can start either NT version. This is not a desired alternative anywhere in the MCEN without specific approval.

(2) Upgrade. The upgrade option is the preferred choice. This will upgrade NT 4.0 and all current settings to an NT 5.0 Active Directory environment. Users will not be able to boot to the old NT 4.0 configuration after the upgrade is complete.

c) Wizard interaction

After the choosing the upgrade option, the wizard copied most of the required files to the hard drive and started an interview process to determine the upgrade configuration. After displaying a list and confirming all hardware resources and peripherals, the wizard started the user-input phase. Some of the more important questions are:

(1) Domain Name. The wizard automatically concatenates the old NT 4.0 domain name with the previous DNS information contained in the TCP/IP property window of the PDC. The wizard then asked if the new NT 5.0 domain name *NT5BETA.nps.navy.mil* was correct. If the NT 4.0 domain name contained characters that were not Internet compliant, the new domain name required modification to comply with Internet rules.

(2) Domain Tree. The wizard then asked if the administrator wanted to join a new domain tree or if the domain would join an existing domain tree. All domain upgrades should choose to join an existing domain tree except for the one PDC at the top-level domain in the MCEN. The parent domain name was entered at this phase.*

(3) Site Name. The next information requested by the wizard was the identity of the NT 5.0 site that the DC would join. Since this DC was the first to upgrade into a new NT 5.0 domain tree, a notional site was created and named *NT Lab.* Because sites are based on physical location and IP subnets, the wizard accepted this information without hesitation.

(4) Promotion. The wizard then notified the administrator that it would automatically promote the NT 4.0 PDC to an NT 5.0 DC with all the appropriate account databases and drivers.

(5) DNS changes. Since an Active Directory DNS server was not used before migration, the wizard prompted the administrator for an IP address of the appropriate DNS server. Since this upgrade simulated the first DC in a new domain tree, an NT 5.0 DNS server could not previously exist. The IP address of the previous DNS server (UNIX) was changed to the IP address of the same DC receiving the upgrade with

---

* Since this test did not have any other NT 5.0 domains to join, a new domain tree was created. When the authors entered a notional domain tree, the wizard tried to contact the parent domain but failed when it could not find it on the network.

the intent to add DNS as an NT 5.0 service after completion. Additionally, the information in the DNS window under TCP properties was changed to *NT5BETA.nps.navy.mil*, reflecting the DNS server installation that would follow the server upgrade.

3. BDC

a) Upgrade BDC to create a domain

Microsoft does not recommend upgrading the BDC until an NT 5.0 DC exists in the domain. The authors tried to upgrade a BDC before the PDC and, as predicted, experienced several problems. Most notably, the upgrade wizards recognized the NT 4.0 DC as a BDC and tried to join an existing NT 5.0 domain. The authors were not given the same menu choices that appeared in the PDC upgrade that would allow the creation of a new Active Directory domain.

Forced to join an NT 5.0 domain, the wizards asked for the name of the Active Directory domain of which the server is a member. Since there were no previous DCs running the Active Directory in order to provide a DNS domain name, the upgrade process could not proceed and the migration failed. Additionally, the authors could not restore the BDC to proper working order and had to reformat and re-install NT 4.0.

b) Upgrading BDC to join a domain

The authors did not execute this type of upgrade due to the lack of available computers. However, Microsoft describes the process as similar to the upgrade process for a PDC. The wizards recognize the computer hardware and ask for

confirmation. An interview process then walks the administrator through a series of questions that include the domain name of the NT 5.0 domain that the DC will join. After the interview process and several re-boots, the BDC will make a successful migration to NT 5.0 and join the previous DC as a peer.

4. Stand-Alone or Member Servers

MCEN administrators use the same procedures to upgrade both the NT 4.0 *Stand-Alone* and *Member* servers. The only difference between the two servers is that the Member server has a computer account in a domain and participates in domain security features while the Stand-Alone is only concerned with local security.

The authors upgraded an NT 4.0 Stand-Alone server to an NT 5.0 Stand-Alone server without incident. Because the upgrade wizards recognized that the server was not a DC and did not participate in a domain, there was no need for the interview phase. After the upgrade to NT 5.0, the server functioned as an NT 5.0 server but lacked many of the tools bundled with the NT 5.0 DCs. At any time in the future, NT 5.0 allows administrators to upgrade the stand-alone server to a DC without re-configuring the system. Changing server roles without re-installation is an added feature of NT 5.0 that did not exist in the previous version.

5. New Installation

While not technically an upgrade, a new installation is another method for creating an NT 5.0 DC. The procedures are very similar as those for the PDC upgrade.

6. Post Upgrade Actions

After the first DC was upgraded, the domain operates in a mixed environment that allows the NT 5.0 DCs to work with other DCs throughout the MCEN while supporting the needs of downlevel clients running NT 4.0. This mixed environment continues until all DCs have received the upgrade to NT 5.0. Once the migration is complete, the administrator can switch to a pure Active Directory domain. Switching to a pure NT 5.0 domain affects only DCs without physically changing domain clients. These legacy clients continue to perform as before but benefit from the changes described below:[23]

- The domain now uses multi-master replication protocol for security
- All downlevel (previous version of Windows) support ceases and NT 4.0 DCs can not be added to the domain.
- All clients now benefit from transitive trusts throughout the enterprise. In a mixed domain environment, some resources belonged to NT 4.0 DCs and do not participate in transitive trust relationships.
- WINS services are required only for downlevel clients.

7. Observations

The wizards presented the authors with several situations that were not predicted in the documentation. The authors upgraded a PDC to an NT 5.0 DC four different times with the same configuration and received similar results. Although instructive, many of the observations noted below will not apply with later releases of NT 5.0 Beta:

- Fast Ethernet (100BaseTX) Network Interface Cards (NICs) are not recognized by NT 5.0.
- NT 5.0 archives DHCP data during upgrade. When DHCP services are validated; the archived data can be deleted.

- PnP worked well on most peripherals, but not with the video and sound card.
- NT 4.0 Domain name was recognized correctly.
- The wizard recommended placing "Active Directory" database and log file on separate hard drives for performance and fault tolerance. Since the test computer only had one SCSI hard drive, this recommendation was not possible.
- The system "froze" on first "Welcome" screen. Re-boot was required.
- Almost all registry settings were carried forward to NT 5.0. The "Shut down" button on the NT 4.0 login screen was disabled during the upgrade.
- Because NT 5.0 did not recognize the PCI NIC, TCP/IP was not installed as a protocol. Therefore, DHCP and WINS did not properly configure on start-up.
- When an older ISA Ethernet (10BaseT) NIC was installed, TCP/IP, DHCP, and WINS were configured without problem
- The final steps included installing and configuring the DNS server. Since Active Directory requires support from an Active Directory compatible DNS server, this is a required step since there were no other DNS options.
- The upgrade to NT 5.0 consumed an additional 115 MB in the Boot partition for a total of 303 MB.
- The normal upgrade required three re-boots of the system. This creates a difficult situation for unattended installations. The Beta 1 version of NT 5.0 does not offer sufficient guidance on how to deal with this problem.
- The PDC should only be upgraded when there is a reliable network connection between the parent domain and the new child. This might pose a significant problem to deployed MCEN units and force them to wait until reliable connectivity is assured.
- The same recommendation applies with regard to connectivity to the designated NT 5.0 DNS server.
- Since NT 4.0 domain names are stored in uppercase letters, the new DNS name of the domain will reflect that same uppercase appearance.
- Changing the IP of the new DNS server before migration helps the upgrade wizard locate the appropriate DNS immediately and makes for a smoother upgrade.

D. MCEN IMPLICATIONS

The MCEN has built a decentralized NT 4.0 enterprise environment. This works well within the Marine Corps culture because all levels of the organization are accustomed to operating under centralized control with decentralized execution. This is true in the execution of the unit mission and the management of NT 4.0 domains. Since the Single Domain is the recommended domain model for each individual unit in the Marine Corps, the MCEN is comprised of hundreds of individually administered domains. While they all follow general guidance promulgated by higher commands, each domain maintains its own security and user policies. These same policies will carry forward into the NT 5.0 environment and it is up to the HQMC to coordinate the overall effects of the MCEN migration.

1. Domain Tree Configuration

As previously discussed, the MCEN should be comprised of only one domain tree and include all USMC organizations in the tree as child domains. This creates a domain tree based on an organizational structure versus a geographical structure. These child domains will maintain the same autonomy they enjoyed with NT 4.0, but the Active Directory features of NT 5.0 will provide interoperability and resource sharing not available with NT 4.0. However the interoperability, resource sharing and directory services come at the cost of increased network traffic. Whenever objects in a domain change, all DCs receive a full copy of the change. If there are *n* DCs, then the Active Directory replicates the change *n* times throughout the domain, regardless of geography. While the other domains do not receive a full copy of the changed object, they still

receive an abbreviated update to their Active Directory. Given the size of the MCEN and the number of Active Directory changes, the MCEN should plan a flexible domain tree structure that maximizes interoperability but minimizes network traffic. Proper site planning and Global Catalog server placement will help increase NT 5.0 benefits while holding down network costs.

*a) **Site planning***

Sites are important to decentralized enterprises such as the MCEN because they control the replication process for DCs throughout the domain tree. IP subnets and physical location define the NT 5.0 site. This helps ensure efficient directory replication and proper management of valuable bandwidth.

Only DCs of the same domain participate in full replication. DCs from different domains in the tree engage in partial replication of tree meta-data so they can reference basic information with regard to enterprise resources. The available network connections between DCs within the domain and those outside the domain determine the desired frequency of the replication. It would not benefit the MCEN to overload a slow Wide Area Network (WAN) connection with Active Directory updates and thus not allow any bandwidth for user data. Microsoft considers a fast network connection to be at least 512 kbps. While this is sufficient for many campus and regional connections, it may not be possible for all MCEN enterprise connectivity. Replication control is a means by which sites can greatly reduce their traffic load.

The MCEN should make extensive use of sites and manage replication according to available bandwidth and the need for critical updates. The default

replication frequency is once every 10 minutes. For slow WAN connections with relatively few directory updates, this frequency can safely be decreased.

A good example of how 1st BN would implement sites is to create them according to buildings in the unit. Since 1st BN uses a star network topology running 10BaseT to all battalion offices, they have a reasonable amount of bandwidth to propagate the replications between sites. However, their barracks is located several miles away and is supported by a DC located in the guard office. This DC receives its updates over a dedicated ISDN connection to another DC in the headquarters building. The administrator would want to decrease the replication frequency for the barracks site from 10 minutes to once every 30 minutes. Replication twice per hour would not overload the 128 kbps bandwidth of the ISDN connection while still providing regular updates to the barracks.

b) Global Catalog servers

Global Catalog servers are specially designated DCs. These DCs maintain a complete Active Directory database for their own domain as well as a partial replica of all objects throughout the entire domain tree. Whenever a client in their domain requests an object that resides in another domain within the tree, the Global Catalog forwards the request based on its domain tree database. Global Catalogs also forward abbreviated object updates from their domain to all other Global Catalogs throughout the domain tree. This allows clients to query local Global Catalogs for enterprise information without requiring DCs to contact each other directly and thus create unnecessary network traffic.

The basic act of implementing Global Catalogs minimizes network traffic because of the partial replication between domains. However, placement of the Global Catalogs is equally important. To minimize inter-domain traffic, the MCEN should employ Global Catalog servers within each NT 5.0 domain. While this will increase the hardware costs and administrative overhead, the reduced traffic over the network and reduced response time for directory queries are valuable benefits.

2. DNS

The MCEN has used DNS names for organizations in the USMC for many years and has created a large decentralized DNS environment with many types of DNS servers. Fortunately, it is not a requirement to replace all existing DNS names or servers in order to make them functional in an NT 5.0 environment.

a) Zones

DNS zone transfer mechanisms allow legacy DNS names and servers to integrate with the NT 5.0 DNS schema. After an NT 5.0 upgrade, the administrator can create a new DNS zone that contains dynamic DNS data on the legacy information. DNS zones correspond to physical locations and can reside at each site if desired. Since many sites already use non-NT DNS servers, this allows both DNS servers to work in parallel. Several benefits of using DNS zones include:[23]

- Less impact on existing DNS services and procedures
- Reduced risk of changing existing DNS structure throughout the enterprise
- DNS servers not fully dependent on Active Directory

The creation of DNS zones has several advantages beyond the above noted benefits. Because DNS zones are organized geographically, the MCEN can create multiple zones based on physical proximity and network topology, thereby reducing replication updates between DNS servers throughout the enterprise. As the MCEN matures the enterprise over several years, it can gradually change DNS names that do not conform to the latest domain name hierarchy without creating widespread disruptions in service and general confusion in the near term.

Administrators must also realize the disadvantages of using DNS zones in a heterogeneous DNS environment. Each DNS zone adds another prefix to the DNS name making the names longer and harder to remember. Additionally, the mixed DNS server network will require integration testing based on the types of legacy systems used with NT 5.0.

Ideally, the MCEN should configure a DNS zone for every NT domain in the enterprise. Additionally, every DNS zone would optimally have a DNS server supporting the Active Directory responsibilities of the DCs.

b) Namespaces

The MCEN has maintained DNS servers for several years but usually only for public access on the Internet. Previously, directory services did not require DNS services within the MCEN and a firewall usually separated the internal resources from external assets. Now that the MCEN will use DNS servers for public Internet access and internal directory services, a namespace solution that is compatible with MCEN firewall (security) practices is required.

One approach to keep internal DNS names secure would be to have a separate DNS naming convention for all Internet resources. This would prevent Internet guests from resolving names inside the Firewall. Unfortunately, this method creates added administration and confusion about proper DNS names for each organization. A better method that maintains the MCEN policy of keeping all internal network assets confidential is the use of identical external and internal DNS names with two different DNS zones for each side of the Firewall. Guests who query the DNS server from the Internet can not resolve names inside the Firewall because they are on a different DNS zone. Figure 17 illustrates a generic company that has the same DNS name on both sides of the Firewall:

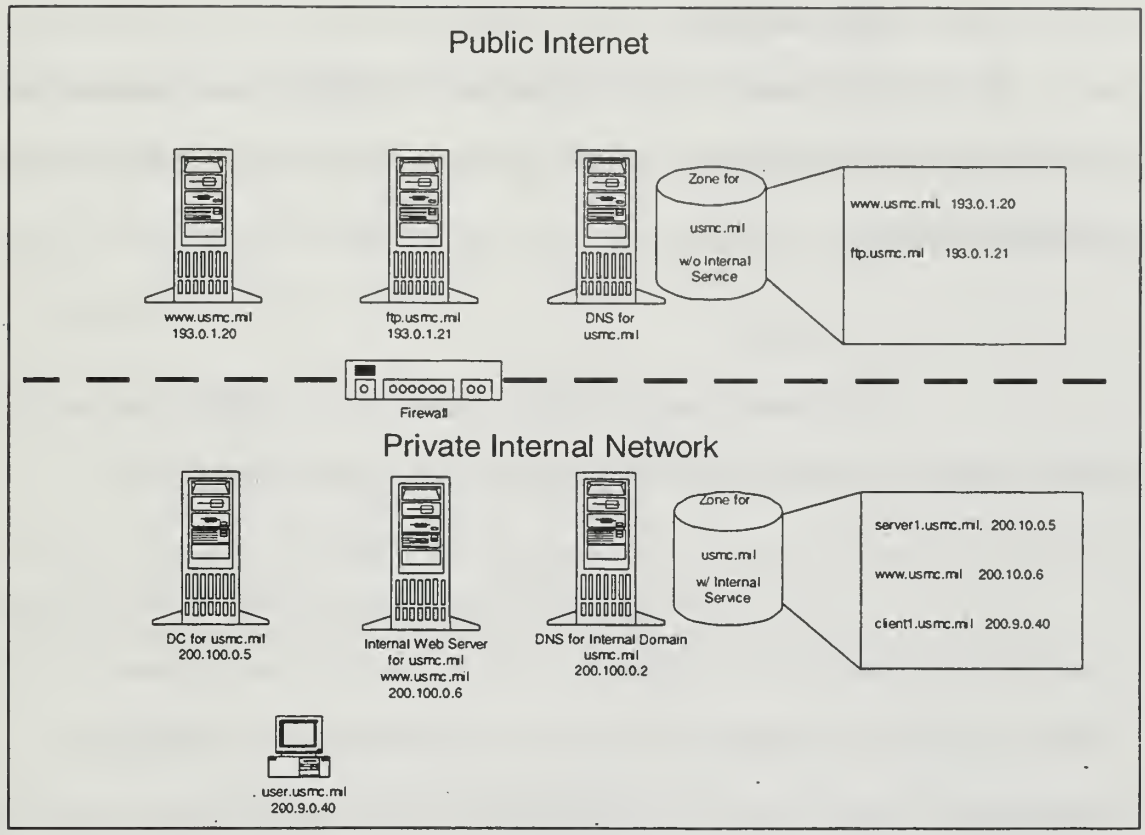

Figure 17. MCEN DNS namespaces

Additionally, MCEN users inside the Firewall have access to internal resources plus Internet assets that are made available. Users would of course realize that their DNS perspective would change depending on which side of the Firewall they access the network. If remote connectivity is required for internal resources, NT services such as Remote Access Service (RAS) and PPTP provides internal access.

3. Active Directory

The Active Directory directly effects how the MCEN should employ DCs and network clients throughout each domain. Some significant effects are discussed in the following sections.

a) DCs

Each domain should maintain at least two NT 5.0 DCs and one NT 4.0 BDC. This will accomplish several important benefits for the domain.

(1) The more DCs that exist in a domain, the fewer clients any one DC is responsible for supporting. This spreads the client requests for Active Directory updates and queries across several machines instead of overloading one. At a predetermined interval, each DC will then replicate any object changes in the Active Directory to other DCs in the domain.

(2) Maintaining both NT 5.0 and NT 4.0 DCs will provide resource access with and without Active Directory. This mixed environment will provide a measure of fault tolerance during the migration and for a period of transition after the upgrade.

b) Clients

After MCEN domains have NT 5.0 implemented in a stable environment, they will want to start upgrading to NT 5.0 on the client. Until that time, MCEN administrators should install the WIN 95/98 client Active Directory tools that are

included with the NT 5.0 installation disk. This will allow the WIN 95 client to browse enterprise resources through Active Directory. NT 4.0 Workstation does not currently have any similar tools and will not run as an Active Directory client. This limitation will require the MCEN to maintain NT 4.0 servers in the enterprise until all NT workstations are upgraded to NT 5.0.

4. NTFS

The MCEN should convert as many NTFS version 4 partitions to the new NTFS version 5 as soon as possible.* Two of the new features most important to the MCEN are the ability to assign disk quotas by user and the ability to encrypt files for storage.

a) Disk quotas

In order to promote the goals of IT-21, The Department of the Navy is encouraging Internet use by all sailors and Marines.[26] While Internet activity is intended to support official needs, users will start significantly increasing the size of cached files in their accounts. Administrators currently have no effective means of preventing one user from consuming more storage space than appropriate. Through disk quotas, NTFS version 5 will provide this valuable capability.

---

* Although the NT 5.0 Beta Release notes caution that NT 4.0 clients can not access the latest NTFS volumes, the authors found that this was not the case. During testing, an NT 4.0 client successfully accessed files on a NTFS version 5 volume residing in the NT 5.0 DC. Additionally, disk quotas were enforced when a user on the NT 4.0 client tried to exceed their allotted disk quota.

b) Encrypting File Systems (EFS)

EFS provides many obvious security advantages. NTFS version 5 will encrypt files at the discretion of the user and protect information from disclosure even if physical safeguards against local intrusion fail. Many security experts and independent studies proclaim that one of the greatest threats to computer security originates from within the organization. Disgruntled employees account for many of the computer crimes that are reported by the commercial sector.[27] While the USMC places extraordinary trust and confidence in its users, history has shown that there are always transgressions.

E. SUMMARY

Migrating to NT 5.0 from NT 4.0 is a complex and time consuming process. The significant improvements to NT 5.0 described in Chapter III require more effort than just a software upgrade. MCEN administrators have to evaluate the structure of the enterprise and make adjustments accordingly. This may require changes in current process and procedures before the migration begins. Upgrading a poorly constructed domain will result in substandard performance. Top down coordination from the NOC is required so that the unit level administrators can effectively execute their own migration process.

V. CHANGE MANAGEMENT

A. DESCRIPTION OF USMC MIGRATION

Thus far, the Marine Corps has focused on the technical changes that NT 5.0 will bring to the MCEN. The goal of this chapter will be to analyze the effects of these changes from a social and managerial perspective. Specifically, we intend to provide some insight on how technical changes within an organization, such as the MCEN, significantly effect the people who work in that organization. These effects can create hostility and resistance to all new initiatives regardless of the reason or source for change. While not all members of the organization will resist change to the same degree, all levels of the organization must anticipate any friction. How well the undesirable effects of change programs are managed often determines the ultimate success of any technical initiative.

1. USMC Organization

The Marine Corps is organized into several broad areas. Two of the major areas are the operational forces, those that carry out the missions, and the support forces, those that that create policy and facilitate the operational forces in conducting the missions. Headquarters Marine Corps (HQMC) is largely concerned with administrative and policy matters. Marine Corps Systems Command (MARCORSYSCOM) at Quantico, Virginia has many duties, one of which is IT policy formulation. The group responsible for Network policy is the NOC.

The operational commands of the Marine Corps are the Fleet Marine Forces (FMF). These forces are responsible for conducting operational missions in support of national security.

2. Migration Strategy Development

The NOC is tasked with coordinating the migration of over 70,000 user accounts and the numerous applications and databases associated with the old Banyan system. Technical milestones were developed to assist in the overall migration effort:

a) Develop migration documentation

A combination of working groups, industry studies, and input from the FMF developed a series of evolutionary documents that guided the USMC throughout the transition. The working groups consisted of technical experts who developed a high leve. view of the technical situation. Included in this group were NOC personnel, Microsoft representatives, and other IT industry representatives. Additionally, the USMC provided in-house experts from various commands.

Best practice analysis was used by the working groups. They conducted site visits to industry leaders in network promulgation and management to determine what parallels could be drawn between other large organizations and the Marine Corps. Specifically, the groups visited Microsoft and Boeing Information Systems.

Finally, when the documentation was drafted it was posted for review on USMC WEB pages for comments from the FMF.

b) Implement the technology

The NOC plans for the technology to be migrated through a sequence of steps; assessment, change and cleanup. Local network administrators will be largely responsible for implementing these steps. NOC training teams will visit major commands for on site assistance. A centralized help desk will also assist users as required.

B. TRANSITION MANAGEMENT

The IT changes will effect every unit and to various degrees, every Marine. The migration approach outlined in the first part of this chapter represents traditional means of achieving change in a hierarchical environment. The NOC conducted careful analysis of the problem and through an iterative process, developed a technically proficient plan for changing the technology or the MCEN. However, for this IT change to be successful, more than just the technology has to change, so do the users. What has been done to prepare the worker for these drastic changes to his familiar and comfortable IT environment? What if the worker has never heard of the NOC and doesn't want to change? What can be done to change his attitudes and perspectives so the technology changes have a better chance of success? To answer these questions, the USMC needs to identify the transition stages for the entire organization including the worker and not just focus on the technology.[28] Several good change models describe the kind of change the Marine Corps can expect.

1. Permanent White Water

The Marine Corps trains everyday to fight on an uncertain battlefield. Leaders at all levels are taught that the battlefield is constantly changing and that they must make rapid decisions based on limited amounts of information. This battlefield chaos is often described as the "fog of war."

The metaphor of "Permanent White Water" describes a similar situation for today's IT managers.[29] Their fog is compared to a rushing river that has a never ending series of rapids. Managers who navigate a boat down this river make sudden and uncertain navigational changes that are very similar to decision making on the battlefield. Each course correction is made with the best available knowledge in a small amount of time. The correction could lead to a successful passage or damage on the river rocks. This comparison is relevant to many Marine Corps managers and leaders. While the Marine Corps trains its leaders to react in a combat environment, many uncertain and critical decision-making situations also exist in a garrison environment (albeit with different consequences). Marines spend countless hours studying the art of maneuver against a well armed enemy, but not much time is devoted to proper decision making in a dynamic support environment such as IT policy development.

2. Endings, Neutral Zone and New beginnings

With each decision and change, there is a period of transition as the organization reacts and adjusts to the change. William Bridges proposes that all organizational transition has three phases that are not very well understood by managers. These phases are *Endings*, *Neutral Zones*, and *New Beginnings*.[30]

a) Endings

This phase launches the transition process. Managers and leaders must realize endings and associated losses will occur no matter how small the change. How the organization copes with the losses will help determine the success of the change.

Every ending is associated with some type of loss. This loss could be the ability to rapidly manipulate an old database or even a reduction in job responsibility due to organizational restructuring. Losses can even occur from positive changes such as promotions. A Lance Corporal who is promoted to Corporal has gained authority but lost peer status with old friends. Losses from endings fall in six categories:

- Loss of Attachments
- Loss of Turf
- Loss of Structure
- Loss of a Future
- Loss of Meaning
- Loss of Control

b) Neutral Zone

Bridges proposes that the least understood phase of transition is the "in-between" time labeled the *neutral zone*. This is when the organization has broken from the old and has not fully implemented the new. Members are many times left to fend for themselves and this can often derail any good transition strategy. Recognizing that this neutral zone will exist the first step in helping people maintain the desired direction. Secondly, supporting people as they navigate through uncertain times is required. This

support includes (1) providing temporary policy and structures that replace any previous loss and (2) continual communication of the organizational objectives. This will help prevent everyone from creating their own individual structure to replace what was lost as the transition started.

c) New Beginnings

Timing is the key to initiating the *new beginning*. People must be in the neutral zone long enough that they are ready to release the old way in favor of the new. Many times, creating dissatisfaction with the old way is the best means to gain acceptance for a new solution that carries out management's transitional intent. However, if the new beginning is presented too late, then people have already developed their own solutions to make up for their losses which may run contrary to management's intent. A case in point is the dissatisfaction Marines feel when trying to work in the Joint arena. The incompatibility of the Banyan Vines systems with those used by the other Services increases the frustration and dissatisfaction they feel. This creates a fertile environment that helps initiate the change that the Marine Corps desires.

3. Communicating The Transition

The USMC has long known the importance of good communications. Many battlefield successes depended on maintaining constant communications with all members of the unit, not only the top decision-makers. The same priority exists for communicating change throughout an organization during times of transition. Communication during the *ending* phase requires managers to explain what, when and

why the change is going to happen. Communicating in the *neutral zone* requires managers to provide people with "...a sense that someone was looking out for them during a very difficult time and that a process of clarification was going on that would in time provide the organization with a new direction."[31] *New beginnings* require communication that is informative and inspirational. When managers pass the message about new beginnings, they are signaling the end of the neutral zone and a time to put the new ideas to work.

C. USMC TRANSITION

The NOC can apply many aspects from the transition examples in the previous section to the NT migration initiative. Since Marines are relatively adept at decision-making in uncertain environments, the rapid change of a white water world is not unduly foreign. But when the NOC migration plan is compared to Bridge's model of Endings, Neutral Zone and New Beginnings, the biggest deficiency is the two way communication that is vital to migration success. Table 3 describes just some of the individuals that will experience endings as described above.

	MCEN	Network Admin. (Unit)	Banyan Corp.	Marine (Worker)
Turf	Conform to DoD standards	Loss of Knowledge Experts are different	USMC is not customer	Expertise ↓ Proficiency ↓
Attachment	Vendor is different	Peers change Experts lost Support different	Reduced commitments Fewer requirements	Training is archaic Help references are lost
Structure	NT not Banyan	Physical configuration Different Reports Unknown maintenance issues	USMC account is gone	No familiar look No Email directory
Future	Microsoft "slave" Loss of uniqueness	Lost billets New experts required	Fewer customers	What next?
Meaning	Obscurity ↓	Confidence ↓	Prestige ↓	Why did we change?
Control	Loss of IT independence	Centralized decisions Power ↓	Market share ↓ Future bleak	Productivity ↓

Table 3. List of Losses

One of the most effective tools to decrease the losses and to help navigate the neutral zone is communication. The Marine Corps and the NOC should have a clear communication plan to support the Banyan-to-NT transition. Currently the NOC is using a variety of methods in communicating intentions but there is no coherent plan to maintain support through the different phases of transition. Even forming a basic plan for conveying the organizational message to all levels would greatly increase the chance of success.

Decker Communications, Inc. of San Francisco has been helping organizations achieve their goals by improving their communications process. They believe that there is no substitute for person-to-person communication. To help organizations share their vision and implement change Decker developed a list of critical success factors. A brief

discussion with one of their consultants revealed how the NOC can apply some of these principles to the NT migration:[32]

1. Communicate Early and Often

Use all available communications channels to support the person-to-person communication. Media options such and videotape, WEB pages, journal articles, etc. are but a few examples the Marine Corps can use to propagate the message and the vision. The focus should be on getting all managers to participate in the message early and as often as possible.

2. Communicate Your Destination

Convey the organization's strategic direction. Create a vivid description of what employees will see, hear, and sense upon arrival at the destination and why the organization is going there. This enables the members to make a conscious decision to personally commit to the goal. The NOC should not only describe the technical end-state but also how it will look. A description of the great improvements that the average user and maintainer will witness once the new beginning arrives will build valuable anticipation such as seamless integration of IT resources in the Joint environment.

3. Create Messages That Motivate

Motivate your listeners by tailoring the message to address their needs, concerns and attitudes. Be specific in what actions the listeners should take, and provide personal benefits to listeners for participating. An effective message should help facilitate attitude and behavioral change. The NOC can challenge all Marines to participate in this service

wide undertaking. Make this an "all hands" event that effects everyone, not just those who administer the system. 100% participation should be the communicated goal.

4. Build Commitment Interactively

Face-to-face communication helps build acceptance and commitment to the goals. Building trust and believability are critical to successful communication. It is important not only to appeal to the intellectual side of the audience, but also to their emotional. The NOC should take every effort to brief the established chain of command and have them conduct a face-to-face brief with their Marines. This would take advantage of the existing relationships at lower levels of management instead of change communicated by strangers.

D. SUMMARY

The Marine Corps is well on its way in developing an effective technical transition strategy for migrating the MCEN to the latest NT system. However, without examining the social interactions inherent whenever technical changes occur, the Marine Corps runs the risk of initiating a major change that is less than optimal. By considering some of the social factors described in this paper, the Marine Corps can develop a robust and effective transition strategy that is not only technically sound, but that is understood, embraced, and executed by those who work in the MCEN.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. NT 5.0 Improvements over NT 4.0

NT 5.0 corrects some of the shortfalls found in NT 4.0 while offering significant enhancements. These enhancements include:

- Active Directory, which provides extensible directory services. Active directory allows for expansion.
- NTFS Version 5 now allows for hard disk space quota assignments for user accounts. It also allows for file encryption.
- Integrated security for authentication and file encryption

2. Centralized Coordination, Decentralized Execution

We need to centrally plan before we act. Training is required to ensure that users and subordinate commands understand the strategy and implement it correctly. However, execution of the strategy should be decentralized, with commands given the authority and flexibility to execute the plan as provided.

3. DII COE Compliance And Joint Interoperability

One of the challenges the Marine Corps faces is interoperability with other forces. IT-21 established Windows NT as the de facto standard for a network operating system. Windows NT is DII COE compliant. Migration to NT will enhance our ability to operate in the joint arena.

B. RECOMMENDATIONS

NT 5.0 was initially scheduled for market release at the end of 1998. However, with the recent release of NT 5.0 Beta version 2, as well as a scheduled release of Beta version 3, it is unlikely that NT 5.0 will hit the market in the near future. Since the release of NT 5.0 is likely to be delayed until the spring of 2000, NOC personnel should reevaluate the migration plan and adjust accordingly. Particular attention should be paid to any problems that might arise as a result of the Y2K dilemma. Since the NOC is implementing Banyan Vines 8.5, this should minimize Y2K problems until the migration to Windows NT is completed.

Major changes within an organization can have a significant effect on personnel. Migrating from Banyan Vines to Windows NT is a significant change. This migration could potentially create upheaval within the data systems community as personnel try to adjust to an unfamiliar network operating system. Power relationships and attitudes of self-worth may be affected as those who were the former "duty-experts" with the old system are now the "neophytes" with the new. Decisions with regard to which personnel get to attend schools or receive training on the new system can have a major impact on morale. Leaders must consider the impact of change within an organization in order to properly plan for the consequences.

C. AREAS FOR FURTHER RESEARCH

1. Evaluating NT 5.0

The authors' original intent was to construct a small enterprise network implementing NT 5.0. However, we quickly found that the Beta version of NT 5.0 did

not provide full functionality and therefore severely restricted our ability to evaluate it. We were further limited in our access to computers that could adequately support NT 5.0 server requirements.

Once NT 5.0 is released, additional research should be conducted to evaluate its capabilities and to test new concepts and features before its implementation into the MCEN. As the release date of NT 5.0 draws closer, other students could contact the NOC to arrange for testing of the new software in a simulated enterprise environment.

2. Certificate Servers in the MCEN

When the authors first contacted the NOC concerning the thesis topic, a plan to implement certificate servers in the MCEN was suggested. Additionally, the issue of public key encryption was also suggested. Use of certificate servers and PKI technology were beyond the scope of this thesis research and as such were not considered. This is, however, a rich area for investigation and thesis research.

3. Security Concerns with NT

Again, analyzing the security flaws associated with the NT NOS went beyond the scope of this research. The importance of security is well understood by the authors and provides another potentially fruitful area for investigation.

4. X.500 Capability for the MCEN

Windows NT uses the LDAP protocol for directory services. While LDAP is based on the X.500 standard, there is some doubt as to how well it will integrate with other X.500 directory services.

As the Marine Corps migrates away from Banyan Vines Street Talk Directory Assistant (STDA), the MCEN must find a suitable replacement. The development of a migration strategy for an interoperable directory service capability for the MCEN is another area for further study.

LIST OF REFERENCES

[1] Joint Chiefs of Staff, *Joint Vision 2010.*

[2] Headquarters Marine Corps, *Operational Maneuver From The Sea*, U.S. Marine Corps, 1995.

[3] Marine Corps Systems Command, Technical Discussion Paper, Revision B, *USMC UNCLASSIFIED NT NOS / EXCHANGE MESSAGING MIGRATION,* 5 May 1998.

[4] Headquarters, Marine Forces Atlantic, http://www.nfd.usmc.mil/.

[5] Headquarters, Marine Forces Pacific, http://www.mfp.usmc.mil/.

[6] I Marine Expeditionary Force, http://158.238.52.76/history.htm.

[7] Network Operations Center, Headquarters Marine Corps, http://www.marcorsyscom.usmc.mil/c4i/pm-sec/noc-dex.html.

[8] NT Server 4 in the Enterprise Study Guide

[9] NT migration

[10] Baltazar, Henry, "NetWare 5.0: Fine for faithful." *PC Week ONLINE,* 7 September, 1998

[11] Yager, Tom, "Windows NT 5.0 Beta," *Windows NT Systems*, February 1998.

[12] www.microsoft.com/ntserver/, July 14, 1998.

[13] "Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services," *White Paper,* Microsoft Corporation, 1997.

[14] Strebe, M., Perkins, C., and Chellis, J., *MCSE: NT Server 4 Study Guide,* 2nd ed., Sybex Inc., 1998.

[15] Janah, Monua, "Enterprise Harmony."InformationWeek, Issue 684, pp. 46-50, 1 June 1988.

[16] "Active Directory Technical Summary," *White Paper,* Microsoft Corporation, 1997.

[17] "Microsoft Windows NT 5.0 Backgrounder," *White Paper,* Microsoft Corporation, 1998.

[18] Brundrett, P., "Kerberos authentication in Windows NT 5.0 domains," *;login:*, May 1998.

[19] Proctor, P.E., "Kerberos in Windows NT 5.0," *NT Systems,* June 1998.

[20] "Encrypting File System for Windows NT Version 5.0," *White Paper,* Microsoft Corporation, 1997.

[21] "Windows NT Version 5.0 Beta 1 Release notes," Microsoft Corporation, September 1997.

[22] "Planning Windows NT Server 4.0 Deployment with Windows NT Server 5.0 in Mind," *White Paper,* Microsoft Corporation, 1998.

[23] Migrating from Microsoft Windows NT Server 4.0 to Windows NT Server 5.0," *White Paper,* Microsoft Corporation, 1997.

[24] Daily, Sean, "Preparing for NT 5.0," Conference notes from *COMDEX Enterprise 98*, San Francisco, 8 September 1998.

[25] "Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services," *White Paper,* Microsoft Corporation, 1997.

[26] "Internet Policy," Naval Message (Department of the Navy, February 21, 1998).

[27] Hutt, A.E., Bosworth, S., and Hoyt, D.B., *Computer Security Handbook*, 3rd ed., John Wiley & Sons, Inc., 1995.
[28] Kotter, John P., *Leading Change*, Harvard Business School Printing, 1996.
[29] Vaill, P.B., *Learning As a Way of Being: Strategies for Survival in a World of Permanent White Water*, Jossey-Bass, 1996.
[30] Bridges, William, *Surviving Corporate Transition : Rational Management in a World of Mergers, Layoffs, Start-Ups, Takeovers, Divestitures, Deregulation, and New Techno*, 1988.
[31] Bridges, William, *Transitions*, Perseus Printing, 1980.
[32] Interview between Sara Watkins, Corporate Communications Consultant, Decker Communications Inc., and the authors, 2 June 1998.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 94943-5101

3. Director, Training and Education 1
   MCCDC, Code C46
   1019 Elliot Road
   Quantico, VA 22134-5027

4. Director, Marine Corps Research Center 2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico, VA 22134-5107

5. Director, Studies and Analysis Division 1
   MCCDC, Code C45
   3300 Russell Road
   Quantico, VA 22134-5130

6. Network Management Branch 2
   Attn: Major Burnette
   Network Operations Center
   2033 Barnett Ave., Suite 315
   Quantico, VA 22134

7. Marine Corps Representative 1
   Naval Postgraduate School
   Code 037, Bldg. 234, HA-220
   699 Dyer road
   Monterey, CA 93940

8. Marine Corps Tactical Systems Support Activity 1
Technical Advisory Branch
Attn: Major J.C. Cummiskey
Box 555171
Camp Pendleton, CA 92055-5080

9. Professor Doug Brinkley 2
Naval Postgraduate School
Code SM/B
Ingersoll Hall
Monterey, CA 93943-5000

10 Professor Bert Lundy 1
Naval Postgraduate School
Code CS/LN
Spanagel Hall
833 Dyer Road
Monterey, CA 93943-5000

11. Major Robert A. Rowlette 2
13 N. Pointe Drive
Fredericksburg, VA 22405

12. Captain Douglas B. Thiry 2
300 Yarmouth Street
Apt. #321
Norfolk, VA 23510

13. Mr. J. K. Thiry 2
1324 Old Saybrook Rd.
Lancaster, PA 17601

14. Ms. Claudine J. Landry 2
1525 Pine Tree Drive
Edgewater, FL 32132

66 553NPS TH 3773
11/99 22527-106 NICB

DUDLEY KNOX LIBRARY
3 2768 00350133 9